

10BaseT - A form of Ethernet and IEEE802.3 network cabling that uses 10 Megabits per second, baseband, twisted pair cabling.

Address Mask - See Subnet Mask.

ARP (Address Resolution Protocol) - Internet protocol uses the IP address to determine the corresponding physical address. Allows a host to find the physical address of a target host on the same physical network, given only the target's Internet address. The sender's Internet-to-physical address binding is included in every ARP broadcast; receivers update the Internet-to-physical address binding information in their cache before processing an ARP packet.

Baseband - A transmission technique used in LANs. One device at a time can communicate, and a device sends its digital signal without modification on the cable.

BootP (Bootstrap Protocol) - A TCP/IP protocol by which a device can obtain such identifying information as its own IP address or download software from a remote server.

Bridge - A special purpose, dedicated computer that connects at the MAC layer two or more segments of the same network and routes packets from one to the other.

Client - An SNMP workstation to which SNMP traps (event messages) are sent.

CSU/DSU - A combination Channel Service Unit/Data Service Unit. A CSU conditions serial synchronous data for transmission over digital networks. The CSU provides such services as transmit and receive filtering, signal shaping and balance, equalization, and loopback testing. A DSU adds bipolar conversion features to improve signal shaping and strength to make transmission virtually error free.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection) - A characteristic of network hardware that operates by allowing multiple stations to contend for access to transmit by listening to see if the line is idle and also allows the hardware to detect when two stations simultaneously attempt transmission.

Datagram (see IP Datagram)

DDD (Direct Distance Dialing) - The public telephone system.

DDS (Digital Data System) - AT&T DDS service and similar digital services operating at 56 kbps.

DLCI (Data Link Connection Identifier) - A frame relay numeric identifier for the local end of a logical circuit.

Dotted Decimal Notation - The representation for a 32-bit integer that consists of four 8-bit numbers written in base 10 with periods (dots) separating them.

Encryption - The conversion of information into unintelligible form (cipher) for security reasons.

Ethernet - A LAN transmission network using a bus structure, first produced by Xerox, later adopted by DEC and Intel, and later adapted to create the IEEE 802.3 and ISO 8802-3 standards.

Flash - A type of non-volatile read-write memory.

Fragment - One of the pieces that results when an IP gateway divides an IP datagram into smaller pieces for transmission across a network that cannot handle the original datagram size. IP software at the receiving end reassembles fragments into complete datagrams.

Frame Relay - A standardized interface specification that provides data transfer between routers over a WAN. Frame Relay is primarily intended for use on high-quality transmission lines, where data is received relatively free of errors. Frame Relay provides data rates of up to 2.048 Mbps. Frame Relay also allows multiple simultaneous data sessions (logical channels) across a single physical interface.

FTP (File Transfer Protocol) - An upper-layer TCP protocol that provides for the transfer of files between two dissimilar machines.

Gateway - A special purpose, dedicated computer that attaches to two or more networks and routes packets from one to the other. A gateway provides protocol conversion of routed information.

Hop Count - A measure of distance between two points in the Internet. A hop count of n means that n gateways separate the source and destination.

ICMP (Internet Control Message Protocol) - An integral part of the Internet Protocol that handles error and control messages. Specifically, gateways and hosts use ICMP to send reports of problems about datagrams back to the original source. ICMP also includes an *echo request/reply* which tests whether a destination is reachable and responding.

Internet Address - The 32-bit (dotted decimal notation) address assigned to hosts on the Internet. Actually assigned to the interconnection of a host to a physical network, the IP address consists of a network portion and a host portion.

IP (Internet Protocol) - A standardized method by which separate networks communicate; the inter-connected network is referred to as the *internet*.

IP Datagram - The basic unit of information passed across the Internet. It contains a source and destination address along with data.

IPX (Internetwork Packet eXchange) - A Novell protocol for Novell LAN communications.

ISDN (Integrated Services Digital Network) - An international digital communications standard that supports voice, data, and image applications using standard interfaces over a single telephone line.

LAN (Local Area Network) - A system for inter-connecting computer equipment within a small geographic area.

Leased lines - Permanent physical connections between two local area networks, which can be established through a DDS network.

MAC (Media Access Control) Layer - The lower of two sub-layers in layer 2 of the OSI seven-layer model.

MTU (Maximum Transfer Unit) - The largest data packet size that can be transferred across a physical network.

Multicast - A technique that allows copies of a data packet to be passed to a selected subset of destinations.

NetBIOS (Network Basic Input Output System) - The standard interface to networks on personal computers.

Numbered link - An IPX RIP network number is assigned to the WAN link.

Packet - The unit of data sent across the network. IP datagrams are often referred to as packets.

PDU (Protocol Data Unit) - Datagrams relating to Logical Link Control (LLC) transmissions.

PING (Packet InterNet Groper) - A technique used in the Internet to test reachability of destinations by sending an ICMP echo request and waiting for a reply.

Port - A logical channel mapped to a device interface; the interface might serve more than one port.

PPP (Point-to-Point Protocol) - A standardized data link level encapsulation protocol used on leased lines and dial-up WAN links.

Proxy ARP - The technique in which a device, usually a gateway, answers ARP requests intended for another by supplying its own physical address. By pretending to be another device, the gateway accepts responsibility for routing packets to it. The purpose of Proxy ARP is to allow a site to use a single IP address with two physical networks.

PVC (Permanent Virtual Circuit) - In frame relay, a logical channel between devices that crosses a frame relay network and is identified at each end by a Data Link Connection Identifier (DLCI).

RIP (Routing Information Protocol) - In IP, a protocol used to exchange routing information between hosts on the Internet. In IPX, a protocol used to exchange routing information in the Novell IPX network environment.

Router - A special purpose, dedicated computer that attaches to two or more networks at the network layer and routes packets from one to the other. A router transmits protocol-specific information.

SAP (Service Advertising Protocol) - Novell's implementation of name service, by which services such as file servers and printer servers announce themselves periodically within an IPX network.

Source Quench - When datagrams arrive too quickly for a gateway or host to process, the datagrams are discarded. Source Quench is a congestion control technique by which a device experiencing congestion sends a message back to the source of the packets causing the congestion requesting that the source either stop or slow down its rate of sending datagrams.

SNMP (Simple Network Management Protocol) - A widely-accepted protocol in the TCP/IP environment that permits the management of devices across the network. In its most basic form, SNMP allows the interchange of information between two locations. It uses UDP as its transport layer and IP address as its network layer. The SNMP management station provides the user with a way to process requests and responses into and out of SNMP protocol.

Static Address - In bridging, a permanently configured address to which frames are forwarded or, optionally, not forwarded.

Static Route - In IP, a permanently configured route between devices; a route might be permanently configured to create a route to a device that does not implement the Routing Information Protocol (RIP), or to reduce the amount of traffic required to exchange routing information.

Subnet Address - An application of the IP addressing scheme that allows a site to use a single IP address for multiple physical networks.

Subnet Mask - A bit mask used in subnetworking to identify which bits in an IP address represent the network number and the host number.

TCP (Transmission Control Protocol) - The Internet standard transport level protocol that provides the reliable, full duplex, stream service on which applications depend. TCP allows a process on one host to send a stream of data to a process on another. It is connection-oriented in the sense that before transmitting data, participants must establish a connection. The Internet protocol suite is often referred to as TCP/IP because TCP is one of the two most fundamental protocols.

Telnet - The Internet standard protocol for remote terminal access. Telnet allows a user at one site to interact with a remote device as if the user's terminal is connected directly to the remote device. Telnet application programs connect to the remote device, then prompt for a login ID and password.

TFTP (Trivial File Transfer Protocol) - A simple protocol that provides for the transfer of files between machines. TFTP lacks the sophistication and error-checking of FTP, and is used for simpler tasks in circumstances where error checking is performed by other applications.

Trace route - This function records (traces) the path to a specified host or gateway.

Trap - An SNMP event message.

TTL (Time To Live) - A technique used to avoid endlessly looping packets. In the Internet, each datagram is assigned a time to live value when it is created. Gateways decrement the time to live field when they process the datagram and discard the datagram if the time to live counter reaches zero.

UDP (User Datagram Protocol) - The Internet standard protocol that allows an application program on one unit to send a datagram to an application program on another unit.

Unnumbered link - No IP network or subnetwork numbers are assigned to the WAN interface. Besides conserving IP address space, unnumbered links also decreases the size of the routing table since no direct routes are created for the WAN ports. This reduces the amount of memory required to hold the routing table and also decreases the amount of bandwidth used to send routing updates.

WAN (Wide Area Network) - A network that provides connection services over a large geographic area.

This appendix provides a reference for basic principles of routing and bridging with the Routermate Plus.

B.1	Local Area Networks	B-2
B.1.1	Ethernet	B-2
B.2	Wide Area Networks	B-3
B.2.1	Point to Point Protocol	B-3
B.2.2	Frame Relay	B-4
B.3	IP Routing	B-6
B.3.1	IP Address	B-6
B.3.2	Subnetworking	B-7
B.3.2.1	Subnet Mask	B-7
B.3.2.2	Class C Subnetworking Using RIP 1 ..	B-8
B.3.2.3	Class C Subnetworking Using Unnumbered WAN Links	B-14
B.3.3	Address Resolution	B-16
B.3.4	RIP	B-18
B.3.5	Types of IP Routes	B-20
B.3.6	IP Filtering	B-22
B.4	IPX Routing	B-23
B.4.1	Frame Types	B-23
B.4.2	Novell Addressing	B-24
B.4.3	Watchdog Spoofing	B-24
B.4.4	RIP	B-26
B.4.5	RIP Filtering	B-28
B.4.6	SAP	B-28
B.4.7	SAP Filtering	B-29

B.1 Local Area Networks

A Local Area Network (LAN) is a group of inter-connected computing devices that are confined to a relatively small physical area. LANs provide for centralized management, resource sharing, and uniformity and compatibility of devices. A LAN is a high-speed network due to the relatively short physical area it occupies, and it is privately owned.

Figure B-1 shows a simple LAN on which several personal computers share a single printer.

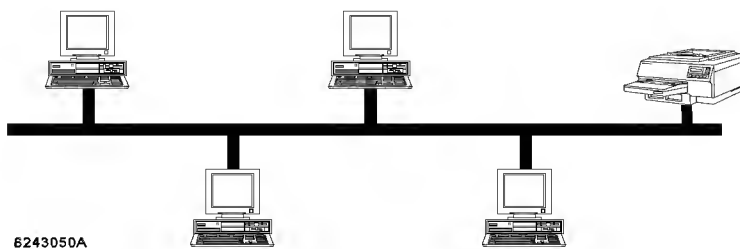


Figure B-1. Local Area Network

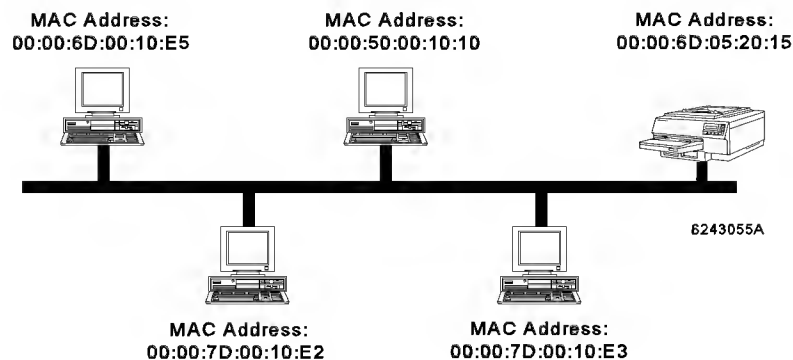


Figure B-2. MAC Addresses on a LAN

B.1.1 Ethernet

Ethernet is a LAN hardware standard that provides for linking up to 1024 nodes (stations) in a bus network. Ethernet uses a baseband (single-channel) communication technique that provides for a 10 Mbps raw data transmission rate. Ethernet uses Carrier-Sense Multiple-Access/Collision-Detection (CSMA/CD) techniques for intra-LAN communication.

Each device manufactured for use on an Ethernet LAN has designed into it during manufacture an Ethernet address, which is also known as the Media Access Control (MAC) address (Figure B-2). The manufacturer assigns the MAC address under the direction of the Institute of Electronics and Electrical Engineering, Inc. (IEEE). Devices on the Ethernet LAN use the MAC addresses to identify and communicate with each other.

B.2 Wide Area Networks

A wide-area network (WAN) provides communication links to remote sites over a public telephone service. There are numerous types of WANs.

Various connect protocols provide standards for the ways in which equipment connects to a WAN. Two connect protocols described below are:

- Point-to-Point (PPP)
- Frame Relay

B.2.1 Point to Point Protocol

The Point-to-Point Protocol (PPP) establishes a synchronous-link connection and encapsulates network-layer protocols for transmission over WAN links.

PPP provides transport services for data packet delivery with low overhead and high throughput. Frame checking at the link level offers error detection; however, error recovery is taken care of by higher layer network protocols.

With PPP, the Link Control Protocol (LCP) establishes, configures, maintains, and terminates the data-link connection.

Various Network Control Protocols (NCPs) manage the specific needs of the associated network-layer protocol.

Reference: RFC 1548, Point-to-Point Protocol (PPP) for the transmission of multi-protocol datagrams over point-to-point links.

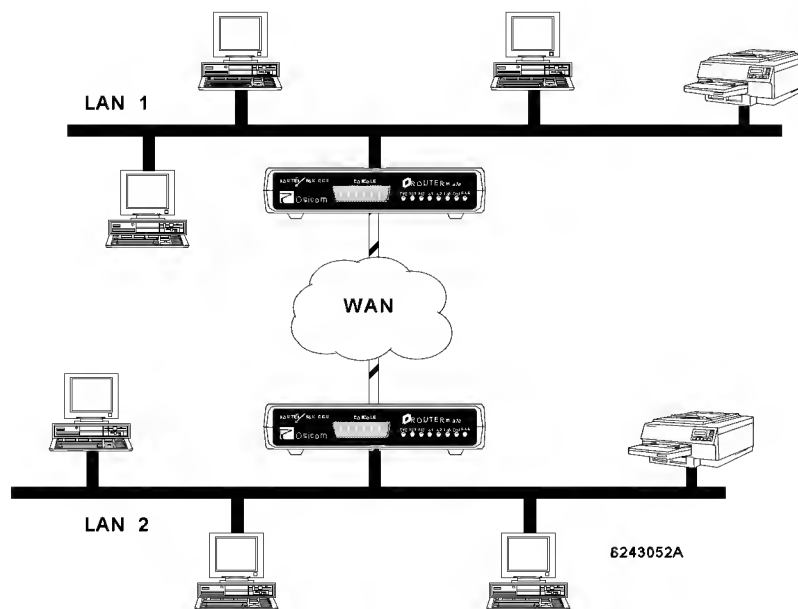


Figure B-3. Wide Area Network

B.2.2 Frame Relay

Frame relay is an interface specification. It provides a mechanism for signaling and data transfer. Frame relay service involves using frame relay access equipment which sends information across the network; this might be, for example, a router, a bridge, a host computer, etc. In public networks, frame relay switching equipment is responsible for the transportation of information across a WAN. Private frame relay switches are required for private frame relay networks.

Frame relay is designed for use on high quality transmission lines. Data is encapsulated according to the Multiprotocol Encapsulation Implementation Agreements of the Frame Relay Forum. Frame Relay accommodates burst-intensive applications, such as wide area LAN inter-connections.

Frame relay provides bandwidth-on-demand and allows multiple simultaneous data sessions (logical channels) across one physical line interface.

Frame relay can be very cost effective when used to interconnect several sites. Frame relay allows several logical links to different sites across one physical connection.

The frame relay network consists of pre-established logical links between the network's endpoints; these logical links are known as Permanent Virtual Circuits (PVCs). Since the links are pre-established, they can be used immediately whenever they are required.

Each PVC on a link is identified logically by a number called the Data Link Connection Identifier (DLCI). DLCIs are obtained from the service provider. DLCIs are used to route frames through the frame relay network. A frame forwarded to the WAN interface is transmitted on the DLCI specified by the port configuration.

The DLCI has local significance only. For configuration purposes, the local user can think of it as identifying a particular destination but, to the network, it identifies a logical connection between the user and the local network access node. It is not a unique address for any specific destination and it can change as the frame travels through the network (see [Figure B-4](#)).

Since the frame relay network is responsible for all switching and routing, a single interface and access line can be used to address traffic to multiple destinations throughout the network.

Figure B-5 compares a PPP application to a similar frame relay application. The PPP application requires four Point-to-Point lines.

The frame relay application requires five (typically less expensive) local-access lines with a single line to each location.

The frame relay application can be more cost-effective since all connections are made through logical links rather than through leased lines.

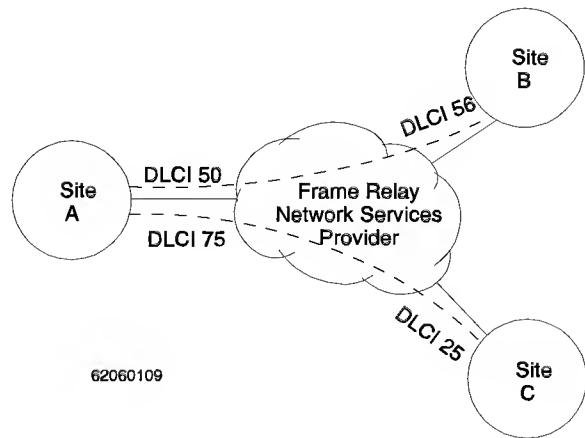


Figure B-4. Frame Relay Network

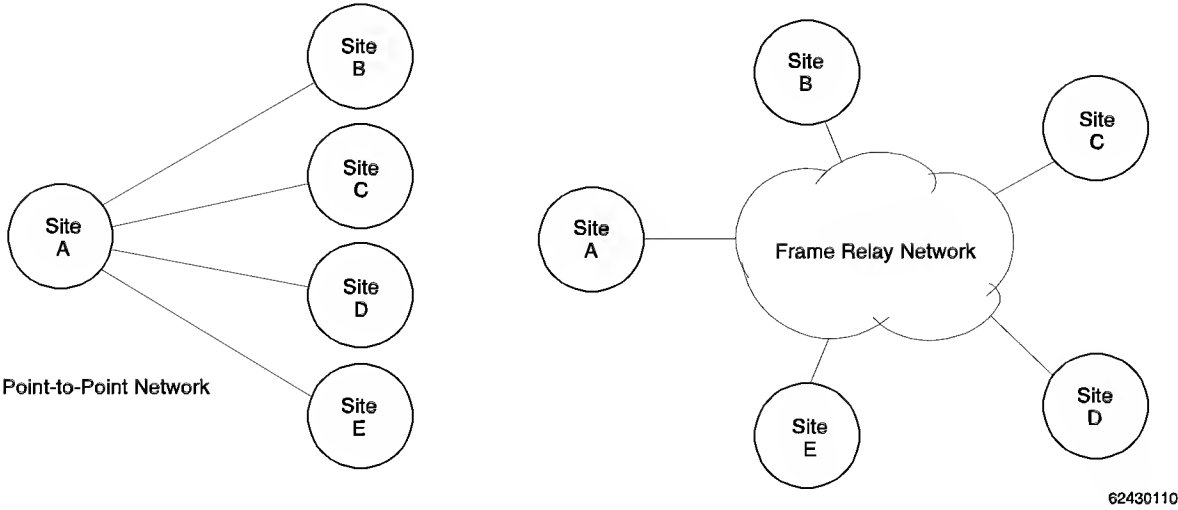


Figure B-5. Point to Point versus Frame Relay Network

B.3 IP Routing

The Internet Protocol (IP) provides a standardized method by which separate networks can exchange information. The Internet Protocol refers to the interconnected networks as the *internet*, and to each communicating device on the internet as a *host*.

Each device communicating on the internet has an IP address, which is also referred to as an *internet address*. More precisely, each host *connection* to a different IP network is assigned an IP address.

B.3.1 IP Address

The IP address is a 32-bit binary number that consists of four octets. An example IP address is:

11000000 00000101 00000011 00010010

Dotted Decimal Notation - For convenience, the value for each octet in the IP address can be written in decimal integers, with the value for each octet separated by a decimal point. Such notation is referred to as *dotted decimal notation*. The expression for the above example IP address in dotted decimal notation is:

192.5.3.18

Network Number and Host Number - IP addresses are divided into two parts: a network number, and a host number.

Internet Address	
Network Number	Host Number

The network number must be unique within internet, and is assigned by the internet service provider under the direction of the InterNIC (Network Information Center) of the Internet Engineering Task Force (IETF). The network number is the same for each device on the network.

The host number must be unique within the local area network. The network owner assigns a unique host number to each device on the network.

Network Size - The network number can be contained in the first, second, and/or third octet of the IP address, depending on the size of the network. Networks are divided into three size classes according to the number of hosts that can be connected to the network:

Network Class	Number of Hosts
Class A	65,636 – 16,777,215
Class B	256 – 65,635
Class C	up to 255

The first three octets in the IP address are used for the network number, as follows:

Class A NNNNNNNN HHHHHHHH HHHHHHHH HHHHHHHH
Class B NNNNNNNN NNNNNNNN HHHHHHHH HHHHHHHH
Class C NNNNNNNN NNNNNNNN NNNNNNNN HHHHHHHH
N=Network H=Host

Class A networks are usually very large networks that contain numerous hosts (or subnetworks). The first octet of the IP address is the network number. This leaves 3 octets for up to 16,777,215 host numbers.

Class B networks are standard, large networks. Class B networks use the first two octets for the network number. This leaves two octets for up to 65,635 host numbers.

Class C networks use three octets for the network number. This leaves one octet for up to 255 host numbers.

Network Class Identification - For all networks, the first two bits in the first octet designate the network class:

Network Class	First Two Bits
Class A	00 or 01
Class B	10
Class C	11

This makes it easy for hosts to recognize the network class. By knowing the network class the host also knows which bits belong to the network number, and which belong to the host number.

Range of Network Numbers - The ranges of numbers that fulfill the above constraints and can, therefore, be assigned in the first octet for each class of network are:

Network Class	Range (Binary)	Range (Decimal)
Class A	00000000 – 01111111	0 – 127
Class B	10000000 – 10111111	128 – 191
Class C	11000000 – 11111111	192 – 255

Additional Addressing Constraints - The following additional constraints also apply to IP addressing:

- For all hosts on the same network, the part of the IP address that makes up the network number is the same.
- A host number of all binary zeroes indicates a broadcast message for all hosts on the network; therefore, a host number of all zeroes is not assigned to a host.
- A host number of all binary ones indicates a multi-cast message; therefore, a host number of all ones is not assigned to a host.

B.3.2 Subnetworking

There are not enough IP addresses to assign an IP address to all of the private LANs and individual hosts on those LANs that would like to communicate on the internet. Subnetworking techniques have resulted from the limited number of available IP addresses. When more than one network is needed, but a limited number of IP addresses are available, the necessary number of networks can be created by organizing a network into subnetworks.

The following sections present a subnetworking method for Class C subnetworking. Although Class A and Class B networks often use subnetworking, the subnetworking methods for these networks are outside the scope of this manual. For a more detailed explanation of subnetworking, the user is referred to any of the widely available texts on TCP/IP.

For a self-contained private network that does not communicate with other IP networks, subnetworking is not necessary. Self-contained private networks can use any valid network addresses and host addresses.

IP networks that communicate with other IP networks can use subnetworking to organize the local network into multiple subnetworks.

B.3.2.1 Subnet Mask

Like the IP address, a subnet mask is a 4-octet, 32-bit binary number that can be expressed in dotted decimal notation. Devices on the network compare the subnet mask to the IP address to derive the network number and the subnetwork number from the IP address.

Only certain numbers can be used as a subnet mask. The subnet mask that is selected pre-determines:

- the number of subnetworks that can be used
- the subnetwork numbers that can be used
- the number of hosts allowed on each subnetwork
- the host numbers that can be used

The subnet mask, therefore, must be selected before IP addresses can be assigned to devices on a subnetwork.

The following are the valid Class C subnet masks that can be used:

Class C Subnet Masks:

255.255.255.192
255.255.255.224
255.255.255.240
255.255.255.248
255.255.255.252

When a device is designed to permit subnetworking, and subnetworking is not used, the subnet mask for the device is configured to indicate a *network mask*, which is the same as *no mask*. The following are the *network mask* configurations for the subnet mask for each network size:

Network Class	Subnet Mask = No Mask
Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

B.3.2.2 Class C Subnetworking Using RIP 1

For the Class C subnetworking method described in this section, Table B-1 shows the following for each of the five valid Class C subnet masks:

- the number of subnetworks that are available
- the number of hosts that can be connected to each subnetwork
- valid subnetwork numbers that can be used with the selected subnet mask
- valid host numbers that can be used for each subnetwork number for the selected subnet mask

In a Class C network, the host number makes up the fourth octet of the IP address. The subnetwork number is not configured as part of the IP address. The device uses the subnet mask and the host number to calculate the subnetwork number.

Table B-1. Valid Class C Subnetworks (1 of 4)				
			Valid Host Numbers	
Valid Subnetwork Numbers				
Number of Hosts per Subnetwork				
Number of Subnetworks				
Subnet Mask				
255.255.255.128	1/2*	126	0*	1 – 126
			128	129 – 254
255.255.255.192	3/4*	62	0*	1 – 62
			64	65 – 126
			128	129 – 190
			192	193 – 254
255.255.255.224	7/8*	30	0*	1 – 31
			32	33 – 62
			64	65 – 94
			96	97 – 126
			128	129 – 158
			160	161 – 190
			192	193 – 222
			224	225 – 254
255.255.255.240	15/16*	14	0*	1 – 14
			16	17 – 30
			32	33 – 46
			48	49 – 62
			64	65 – 78
			80	81 – 94
			96	97 – 110
			112	113 – 126
			128	129 – 142
			144	145 – 158
			160	161 – 174
			176	177 – 190
			192	193 – 206
			208	209 – 222
			224	225 – 238
			240	241 – 254

* Only when Subnet Zero is enabled (see [IP Global Configuration screen](#) on [page 5-44](#)).

Table B-1. Valid Class C Subnetworks (2 of 4)				
Valid Subnetwork Numbers				Valid Host Numbers
Number of Hosts per Subnetwork				
Number of Subnetworks				
Subnet Mask				
255.255.255.248	31/32*	6	0*	1 – 6
			8	9 – 14
			16	17 – 22
			24	25 – 30
			32	33 – 38
			40	41 – 46
			48	49 – 54
			56	57 – 62
			64	65 – 70
			72	73 – 78
			80	81 – 86
			88	89 – 94
			96	97 – 102
			104	105 – 110
			112	113 – 118
			120	121 – 126
			128	129 – 134
			136	137 – 142
			144	145 – 150
			152	153 – 158
			160	161 – 166
			168	169 – 174
			176	177 – 182
			184	185 – 190
			192	193 – 198
			200	201 – 206
			208	209 – 214
			216	217 – 222
			224	225 – 230
			232	233 – 238
			240	241 – 246
			248	249 – 254

* Only when Subnet Zero is enabled (see [IP Global Configuration screen](#) on [page 5-44](#)).

Table B-1. Valid Class C Subnetworks (3 of 4)				
Valid Subnetwork Numbers				Valid Host Numbers
Number of Hosts per Subnetwork				
Number of Subnetworks				
Subnet Mask				
255.255.255.252	63/64*	2	0*	1, 2
			4	5, 6
			8	9, 10
			12	13, 14
			16	17, 18
			20	21, 22
			24	25, 26
			28	29, 30
			32	33, 34
			36	37, 38
			40	41, 42
			44	45, 46
			48	49, 50
			52	53, 54
			56	57, 58
			60	61, 62
			64	65, 66
			68	69, 70
			72	73, 74
			76	77, 78
			80	81, 82
			84	85, 86
			88	89, 90
			92	93, 94
96	97, 98			
100	101, 102			
104	105, 106			
108	109, 110			
112	113, 114			
116	117, 118			
120	121, 122			
124	125, 126			

Table B-1. Valid Class C Subnetworks (4 of 4)				
Valid Host Numbers				
Valid Subnetwork Numbers				
Number of Hosts per Subnetwork				
Number of Subnetworks				
Subnet Mask				
255.255.255.252	63/64*	2	128	129, 130
			132	133, 134
			136	137, 138
			140	141, 142
			144	145, 146
			148	149, 150
			152	153, 154
			156	157, 158
			160	161, 162
			164	165, 166
			168	169, 170
			172	173, 174
			176	177, 178
			180	181, 182
			184	185, 186
			188	189, 190
			192	193, 194
			196	197, 198
			200	201, 202
			204	205, 206
			208	209, 210
			212	213, 214
			216	217, 218
			220	221, 222
224	225, 226			
228	229, 230			
232	233, 234			
236	237, 238			
240	241, 242			
244	245, 246			
248	249, 250			
252	253, 254			

* Only when Subnet Zero is enabled (see [IP Global Configuration screen](#) on [page 5-44](#)).

Figure B-6 shows an example of Class C subnetworking using RIP 1. See page B-14 For an [example](#) of Class C subnetworking using unnumbered links.

In Figure B-6, the IP address assigned by the service provider is a Class C address. It can be recognized as a Class C address because the number in the first octet (192) is within the range for Class C networks (192 through 255).

Since seven subnetworks are required (four for the different sites and three for the links between sites) a subnet mask must be selected that permits at least seven subnetworks. The first subnet mask in Table B-1 that permits at least seven subnetworks is 255.255.255.224. This subnet mask permits up to seven subnetworks (8 when Subnet Zero is enabled) and up to 30 hosts on each subnetwork.

It is good practice when selecting subnetwork numbers to look at the subnetwork topology as a tree, and to assign the lowest subnetwork number at the top of the tree and increasingly higher numbers to the lower branches. For this reason, the first subnetwork number assigned in the figure is subnetwork 32. In Table B-1, it can be seen that hosts on subnetwork 32 for subnet mask 255.255.255.224 can be numbered 33 through 62 (details from Table B-1 for subnet mask 255.255.255.224 are reprinted on this page for convenient reference). If either of the three routers on subnetwork 32 receives information that is to be routed to any host with a host number of 33 through 62, the router uses the subnet mask to calculate that this host is located on subnetwork 32.

In Figure B-6, note the following:

- The IP address assigned to the interface noted in the figure as leading "To Internet" is not part of any of the subnetworks. This IP address is on the service provider's network, and has the service provider's network number.
- The single IP address assigned by the service provider to the customer is assigned to the first LAN interface from the top in the figure. Note that, for this IP address, only the network number is assigned by the service provider.

- Seven subnetworks are required. Four subnetworks (subnetworks 32, 128, 160, and 224) can contain hosts in addition to the router interfaces on each subnetwork. Three subnetworks (subnetworks 64, 96, and 192) are required to address the links for router interfaces between different subnetworks.
- All subnetworks in the example have the same network number (192.3.5.0), which is the network number assigned by the service provider.
- The subnetwork number is not configured in dotted decimal notation as part of the IP address, but is extrapolated from the subnet mask and the host number.
- Each interface for each router connects to a different subnetwork.
- Hosts on a LAN that is located between the interfaces of two connected routers would be on the same subnetwork as the two router interfaces (see subnetworks 32, 128, 160, and 224).

Example: Subnet Mask 255.255.255.224 (part of Table B-1)				
			Valid Host Numbers	
Valid Subnetwork Numbers				
Number of Hosts per Subnetwork				
Number of Subnetworks				
Subnet Mask				
255.255.255.224	7/8*	30	0*	1 – 31
			32	33 – 62
			64	65 – 94
			96	97 – 126
			128	129 – 158
			160	161 – 190
			192	193 – 222
			224	225 – 254

* Only when Subnet Zero is enabled.

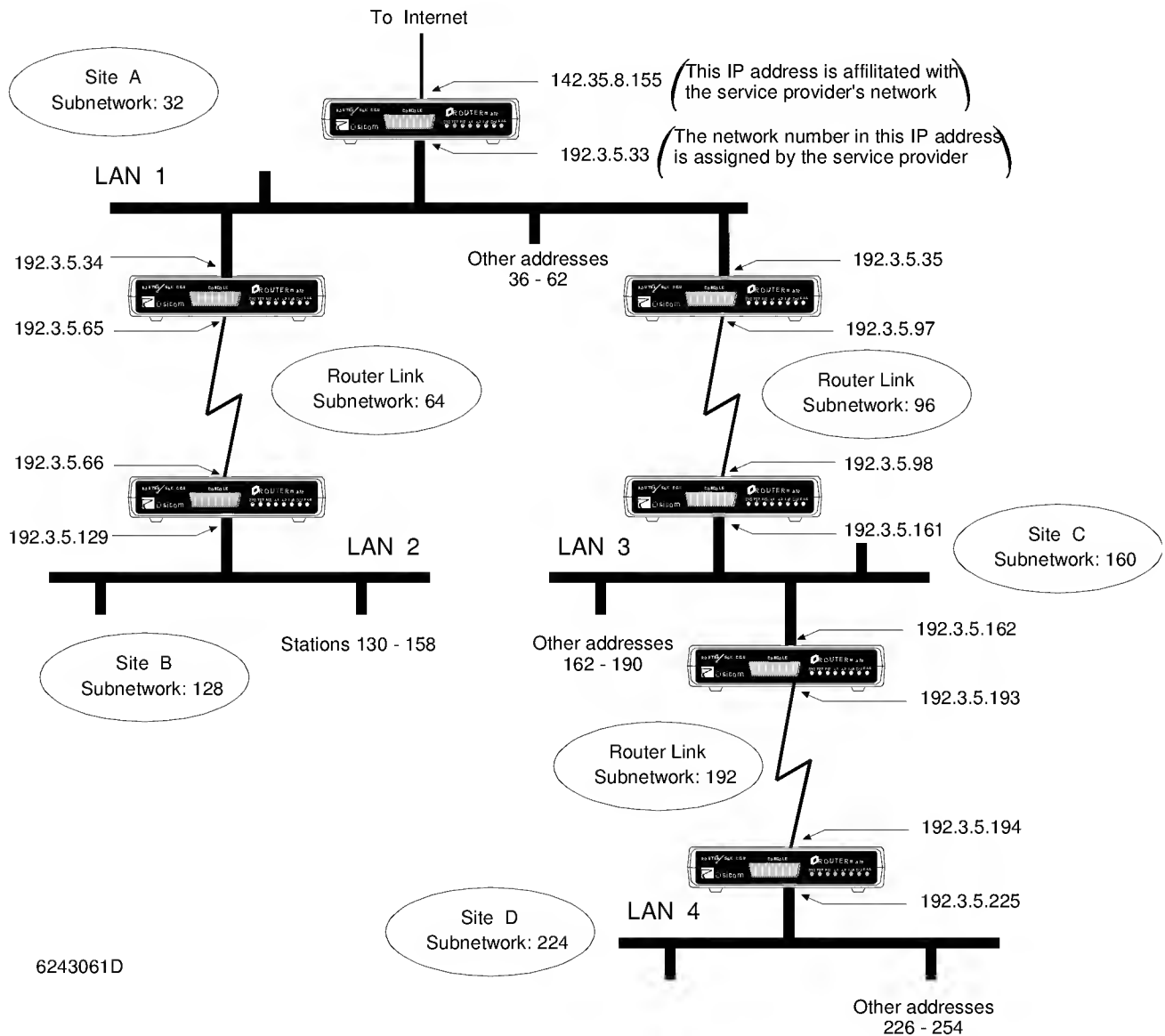


Figure B-6. Class C Subnetworking Example Using RIP 1

B.3.2.3 Class C Subnetworking Using Unnumbered WAN Links

Figure B-7 shows an example of Class C subnetworking using Unnumbered WAN links. See page B-12 for an [example](#) of Class C subnetworking using RIP 1.

In Figure B-7, the IP address assigned by the service provider is a Class C address. It can be recognized as a Class C address because the number in the first octet (192) is within the range for Class C networks (192 through 255).

Since four subnetworks are required (for LANs 1-4) a subnet mask must be selected that permits at least four subnetworks. The first subnet mask in Table B-1 that permits at least four subnetworks is 255.255.255.192. This subnet mask permits four subnetworks (when Subnet Zero is enabled). No addresses are required for the links between sites. Remember to consider future growth needs. Select the subnet that allows the maximum number of stations on each segment.

It is good practice when selecting subnetwork numbers to look at the subnetwork topology as a tree, and to assign the lowest subnetwork number at the top of the tree and increasingly higher numbers to the lower branches. For this reason, the first subnetwork number assigned in the figure is subnetwork 0. In Table B-1, it can be seen that hosts on subnetwork 0 for subnet mask 255.255.255.192 can be numbered 1 through 62 (details from Table B-1 for subnet mask 255.255.255.192 are reprinted on this page for convenient reference). If either of the three routers on subnetwork 0 receives information that is to be routed to any host with a host number of 1 through 62, the router uses the subnet mask to calculate that this host is located on subnetwork 0.

In Figure B-7, note the following:

- The IP address assigned to the interface noted in the figure as leading "To Internet" is not part of any of the subnetworks. This IP address is a numbered link on the service provider's network, and has the service provider's network number.

- The single IP address assigned by the service provider to the customer is assigned to the first LAN interface from the top in the figure. Note that, for this IP address, only the network number is assigned by the service provider.
- Four subnetworks are required. Four subnetworks (subnetworks 0, 64, 128, and 192) can contain hosts in addition to the router interfaces on each subnetwork. When running Unnumbered Links, no addresses or subnets are used by WAN interfaces.
- All subnetworks in the example have the same network number (192.3.5.0), which is the network number assigned by the service provider.
- The subnetwork number is not configured in dotted decimal notation as part of the IP address, but is extrapolated from the subnet mask and the host number.
- Each interface for each router connects to a different subnetwork.
- Hosts on a LAN that is located between the interfaces of two connected routers would be on the same subnetwork as the two router interfaces (see subnetworks 0, 64, 128, and 192).

Example: Subnet Mask 255.255.255.192 (part of Table B-1)				
				Valid Host Numbers
Valid Subnetwork Numbers				
Number of Hosts per Subnetwork				
Number of Subnetworks				
Subnet Mask				
255.255.255.192	3/4*	62	0*	1 – 62
			64	65 – 126
			128	129 – 190
			192	193 – 254

* Only when Subnet Zero is enabled.

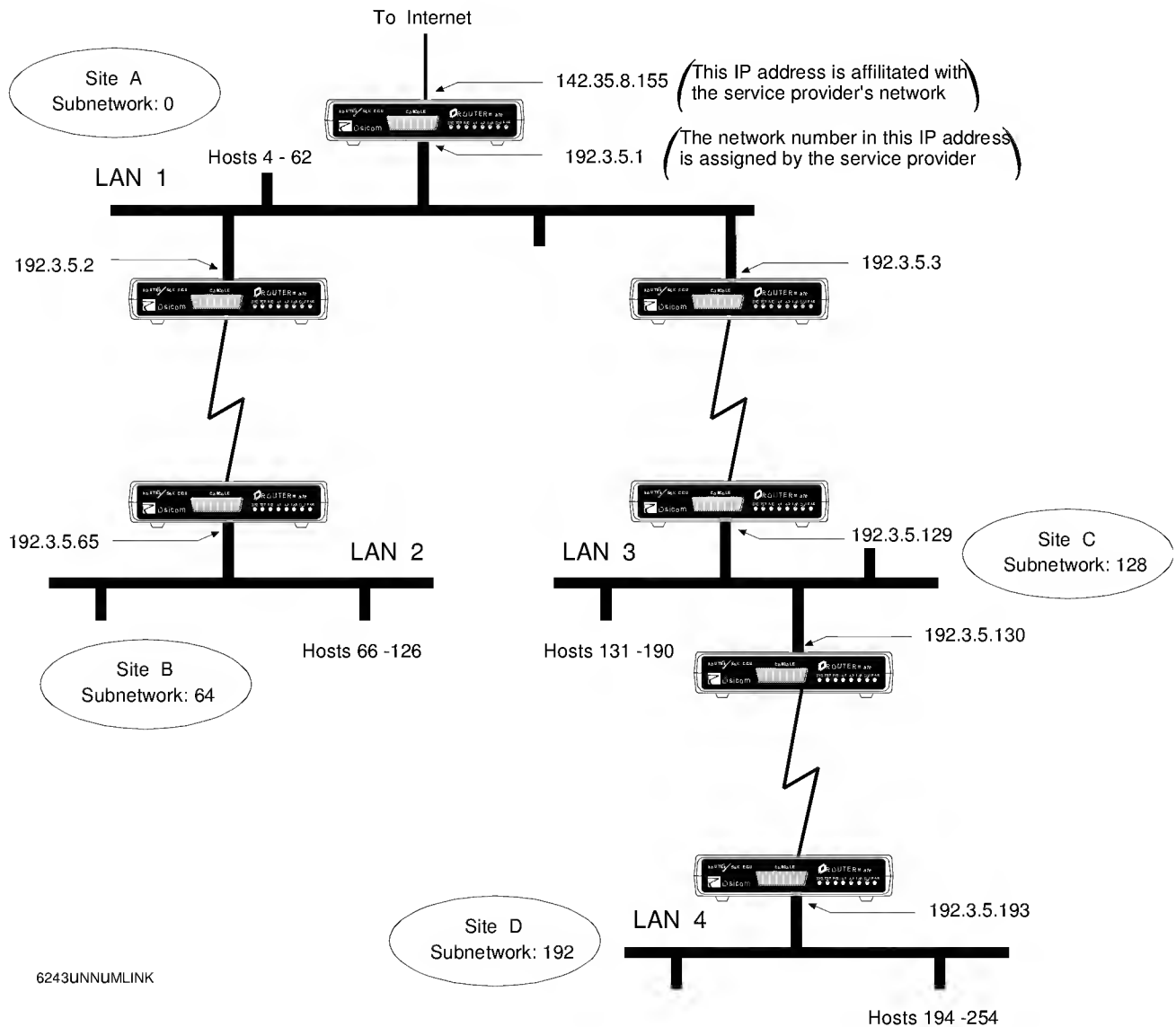


Figure B-7. Class C Subnetworking Example Using Unnumbered WAN Links

B.3.3 Address Resolution

The final communication to any host uses the host's physical hardware address, not the IP address. For an Ethernet LAN, the physical hardware address is the MAC address.

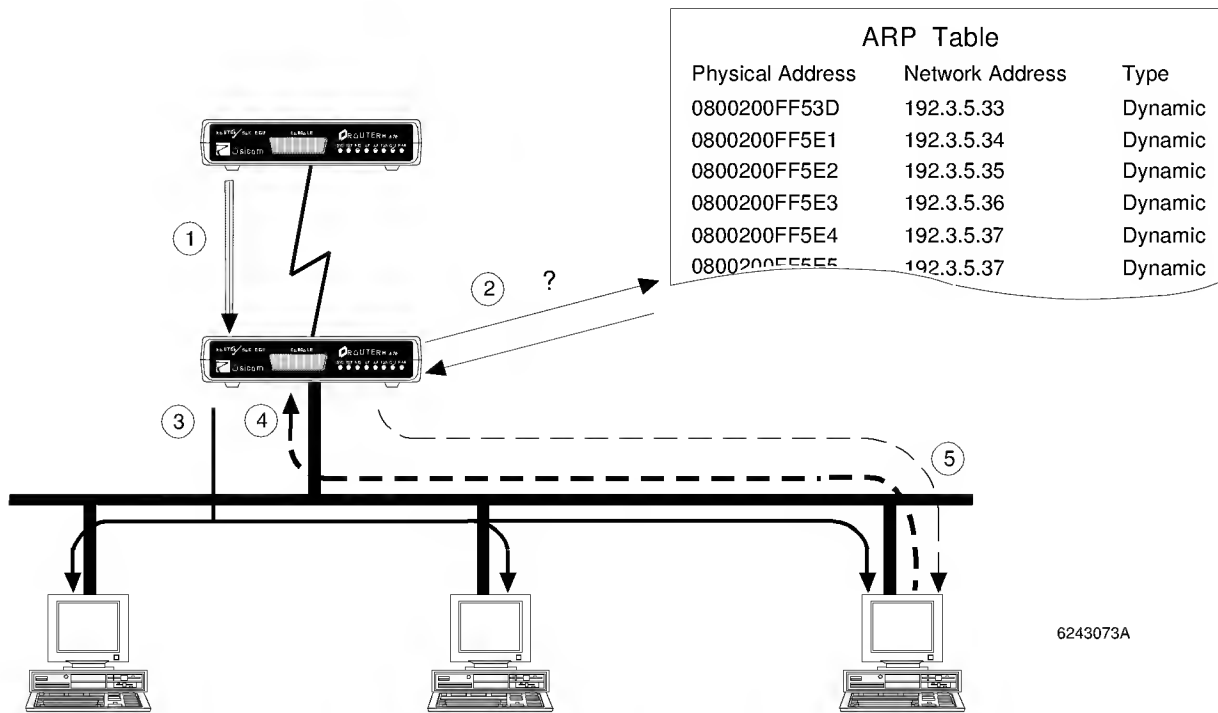
In the router, the MAC address of a host on the LAN is not permanently mapped to the device's IP address. Instead, the router uses the Address Resolution Protocol (ARP) to determine the MAC address. IP addresses and MAC addresses for devices with which the router has communicated recently are retained in the router's ARP table. By referring to the ARP table before broadcasting an ARP request, the router is required to send fewer ARP requests.

The process is shown in five steps in Figure B-8, as follows:

1. The local router receives an IP packet that contains an IP address for a local host.
2. The router checks its ARP table for a MAC address that is associated with the received IP address. If the MAC address is in the ARP table, the router routes the packet to the correct MAC address (Step 5.)
3. If the MAC address is not in the ARP table, the router broadcasts an ARP request to all local hosts. The request includes the IP address for which a MAC address is needed.
4. Only the host with the specified IP address replies. The unknown host sends a reply ARP packet that contains its MAC address.
5. The router then forwards the packet to the host.

All addresses in the ARP table are learned dynamically through ARP requests and replies. As the table grows, few ARP messages are required unless a new host is added or a device's Ethernet card is replaced.

The ARP table can contain approximately 2000 addresses.

**Figure B-8. Packet Delivery Using ARP**

B.3.4 RIP

Routers in an IP environment use the Routing Information Protocol (RIP) to exchange routing information.

A router maintains a routing table that contains routing information for the entire network topology and is used to inform other routers about the network topology.

Each router advertises only to its adjacent routers. RIP messages advertise the information in the routing table to adjacent routers, and request information from adjacent routers, as follows:

- Upon power-up, an initial broadcast informs adjacent routers of networks that can be reached through the router.
- Upon power-up, an initial broadcast requests that adjacent routers provide routing information.
- Periodic broadcasts inform adjacent routers of current routes.
- A network topology change triggers an update to adjacent routers of current routes.

The routing table lets the router:

- Locate the fastest route.
- Retrieve routing information from other routers.
- Respond to requesting routers.
- Advertise the latest internetwork configuration.
- Advertise internetwork topology changes.

If a router does not receive an update for a route after a specified time, the router deletes the route from its routing table, marks the route as unusable, and broadcasts the revised current table to adjacent routers.

RIP describes the distance between a router and a destination network in *hops*. A network immediately adjacent to the local router is 1 hop away, a network that is reached by passing through 2 routers is 2 hops away, and so on.

Each router sends RIP messages that advertise the paths to networks that can be reached via that router. Information in the RIP messages includes, for each destination network, such routing information as the IP network number of the destination network, the number of hops to the network, and the *next hop* IP address (the address of the next router to which packets are sent).

Figure B-9 illustrates a single network (Network A) that consists of four LANs connected by routers; the network is organized into seven subnetwork (4 LANs plus 3 router links).

Subnetwork information is routed only within the subnetwork. In the figure, Router 1 advertises only Network A to the Internet, and advertises the Internet to routers connected to Subnet 1.

As seen in the figure, each router advertises only to its adjacent routers. For example, Router 5 advertises only to Routers 4 and 6.

Routers receiving the RIP messages update their routing tables accordingly and advertise to routers adjacent to them. The cumulative effect is that each router advertises to its neighbors all networks that can be reached through the router.

A path to a network (or subnetwork) that is learned over a particular interface is not advertised back over the same interface, since this would be redundant. For example, Router 2 advertises to Routers 1 and 4 only its paths to Subnets 2 and 3. To Router 3, however, Router 2 advertises its paths to the Internet and to Subnets 1, 4, 5, 6, and 7.

Devices other than routers can receive messages and use them to update their routing tables, but only routers advertise their routes.

Novell IPX networks also use a Routing Information Protocol. The RIP used by IP is different from the RIP used by IPX, although the purposes of both are similar.

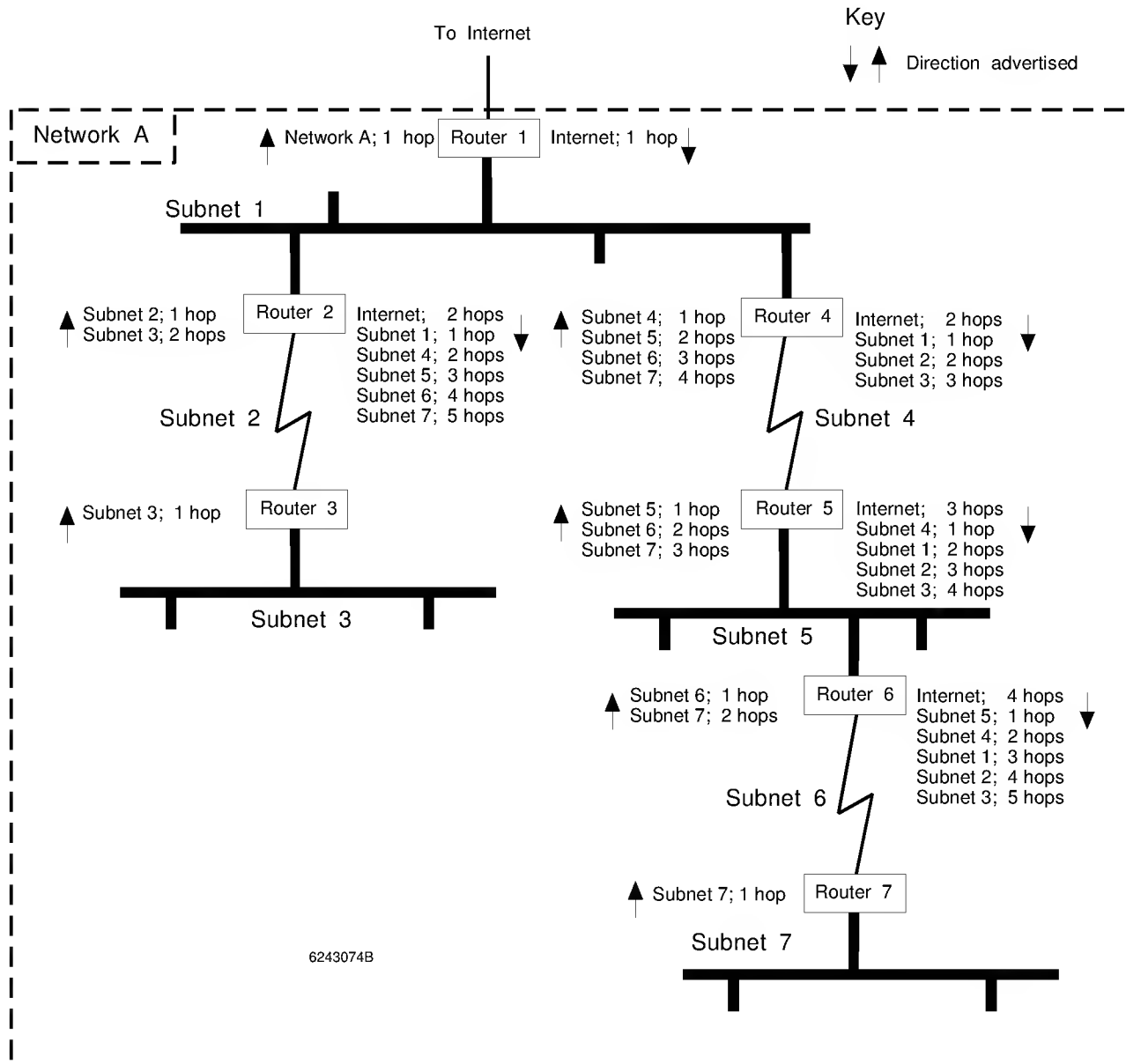


Figure B-9. RIP Advertising Example

B.3.5 Types of IP Routes

There are three types of IP routes:

- *Direct* - The source router is directly connected to the destination network.
- *Static* - A permanently-configured route.
- *RIP* - A route that is learned from a RIP update packet.

Default Route - A fourth type, a *default* route, is actually a static route that is permanently configured for a specific purpose: if a received packet is destined for a network that is not listed in the router's routing table, the packet can be forwarded to a default route.

Direct and Learned Routes - Figure B-10 illustrates directly-connected and learned routes.

In the figure, the path between Router 1 and Router 2 is direct, and the path between Router 2 and Router 3 is direct. Routers 1 and 3 can learn about each other only by receiving RIP update packets from Router 2, so the paths between Routers 1 and 3 are learned.

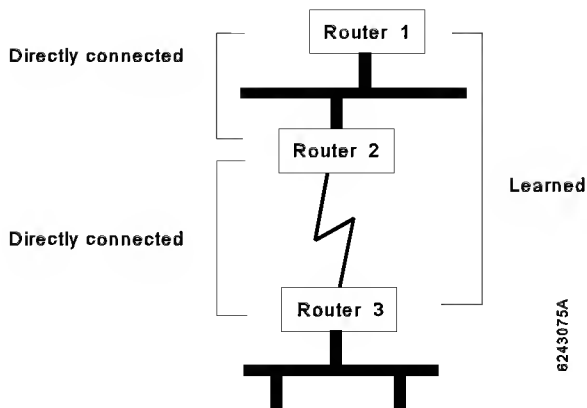


Figure B-10. Direct and Learned Routes

Static Routes - A static route can be created when the router cannot dynamically build a route to the destination, or when it is desirable to reduce traffic over a slow, expensive link.

In Figure B-11, a remote device connected over a WAN link is being booted through the router. A static route must be assigned to the network of the device being booted.

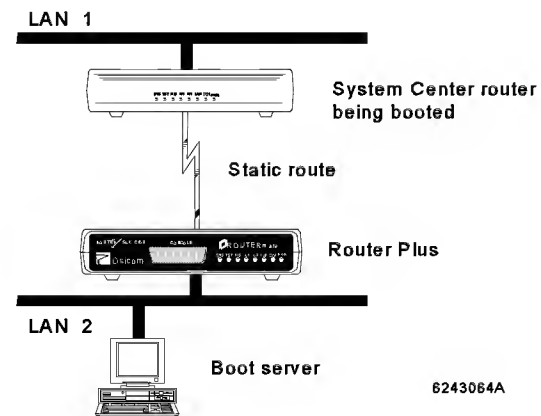


Figure B-11. Static Route to a Remotely-Booted Device

In Figure B-12, LAN 2 and LAN 3 wish to connect to internet networks 126.0.0.0, 17.0.0.0, and 75.0.0.0, but Router 1 does not run RIP.

A static route must be created for routers 2 and 3 to networks 126.0.0.0, 17.0.0.0, and 75.0.0.0. Routers 2 and 3 will then use RIP to announce these static routes, which will let routers 4 and 5 know that the routes are available. LANs 2 and 3 can then reach the three networks.

A static route is floating. That is, if another route with a lower metric is available to the destination, the route with the lowest metric is taken. The metric for a static route is assigned a value of 1 by default and can be re-configured for a value of 1 through 15.

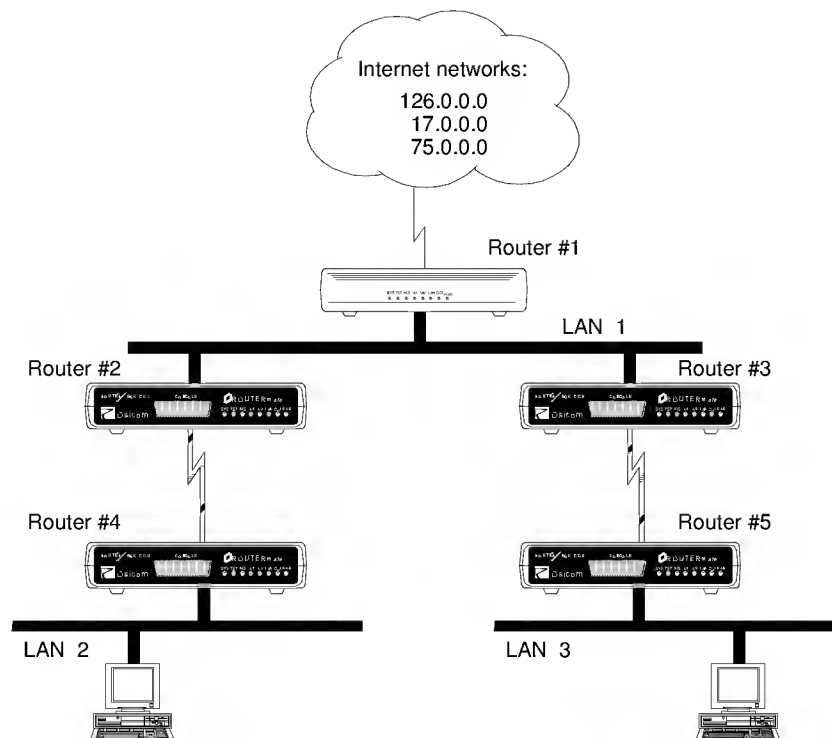


Figure B-12. Static Route to a non-RIP Router

B.3.6 IP Filtering

IP traffic can be filtered to keep certain types of routing information from being received or advertised.

For example, this might be done to:

- restrict access between certain networks
- reduce the amount of routing information traffic (a particularly desirable feature when communicating over packet switched networks)

Ways in which a router might be configured to filter IP traffic could include such filtering as the following:

- Disabling the announcement of static routes, and the default route.
- Receiving (listening to) RIP update messages, but not advertising its own routes.
- When subnetworking is used, a router can (and typically should) be set to advertise only the parent network address of IP subnetworks to other IP networks.
- Specifying addresses from which RIP update packets will or will not be accepted.
- Specifying addresses to which RIP update packets will or will not be sent.

B.4 IPX Routing

The most common type of LAN management software is Novell's NetWare. Novell uses an Internetwork Packet Exchange (IPX) protocol for LAN communications. IPX defines addressing schemes for internetwork and intra-node communications.

Novell IPX routing is based upon IPX Routing Information Protocol (RIP) and Service Advertising Protocol (SAP).

Novell IPX calculates the best route to a destination based upon routing time delays associated with the links and with the number of hops (intermediate routers) taken to reach a network.

Novell IPX RIP is not the same as IP RIP, although the purposes of both are similar.

B.4.1 Frame Types

A router must be configured to recognize which of several IPX frame types is used on the Novell LAN.

Figure B-13 illustrates several IPX frame types:

Ethernet 802.2 (RAW)
 Ethernet 802.3 (LLC)
 Ethernet Type II
 Ethernet SNAP

Except for the IPX Frame Header, each type of IPX frame is composed of a consistent number of fields and bytes. However, for each IPX frame type the IPX Frame Header varies in the number of bytes and the number of fields in the header.

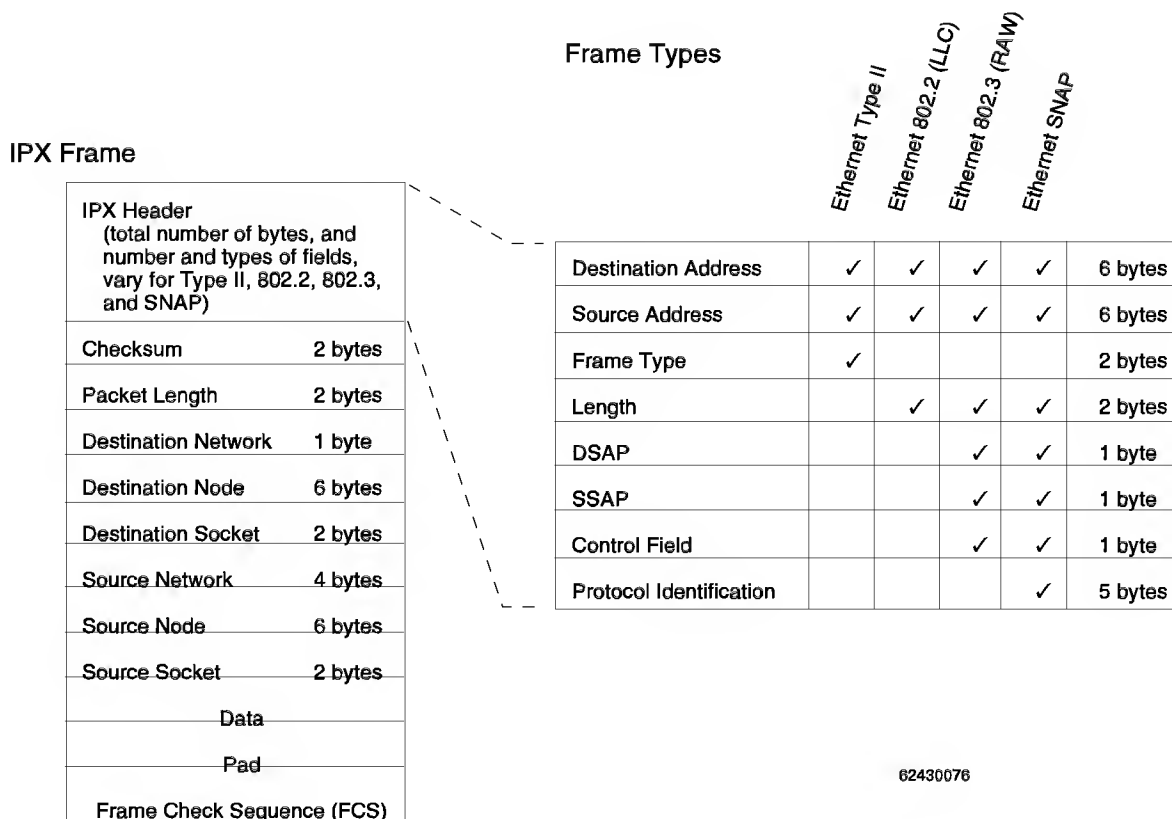


Figure B-13. IPX Frame Types

B.4.2 Novell Addressing

A Novell IPX address is written in hexadecimal notation. It consists of a 4-byte network number, followed by a 6-byte node ID, and a 2-byte socket number.

For example:

00000001 000080123403:0451.

The numbers in the example are:

Network number: 00000001
Node ID: 000080123403
Socket number: 0451

Network Number: A globally unique network number is assigned to each network interface of a Novell server. Servers and router interfaces attached to the same physical network must be configured with the same network number. To simplify network management, only servers and routers must be configured with a network number; workstation's network numbers are assigned automatically by the server (connection to local server) or router (connection to remote server).

Node ID: The Node ID is the MAC address for the device. It is incorporated automatically by software into the IPX address.

Reserved Socket numbers: The following sockets are reserved by Novell:

File Servers:

Socket	Description
451h	NCP process

Routers:

Socket	Description
452h	SAP process
453h	RIP process

Workstations:

Socket	Description
455h	Novell NetBIOS Process
456h	Diagnostics process
4000h to 7FFFh	Dynamically assigned sockets used by workstations for interaction with file servers and other network equipment
8000h to FFFFh	Other sockets assigned by Novell

NCP=Netware Core Protocol
SAP=Service Advertising Protocol
RIP=Routing Information Protocol

B.4.3 Watchdog Spoofing

A Novell file server keeps a table of when client sessions are established and terminated.

When a client has not communicated with a server in a pre-defined time, the server sends a *watchdog packet* to the client to ask if the client still is connected. If a client fails to respond to a pre-defined number of watchdog packets, the session is terminated at the server.

When communication between a number of clients and a server is over an on-demand WAN link, the link never gets a chance to be inactive, and operating costs are high (Figure B-14). Also, if the WAN link is brought down for some other reason, the client sessions might be terminated prematurely.

To counteract the problem of sending watchdog packets over on-demand WAN links, watchdog spoofing can be enabled for the router situated before the WAN link on the server's side (Figure B-15). The router then answers watchdog packets on behalf of clients. This prevents the WAN link from being activated just to send watchdog packets to clients.

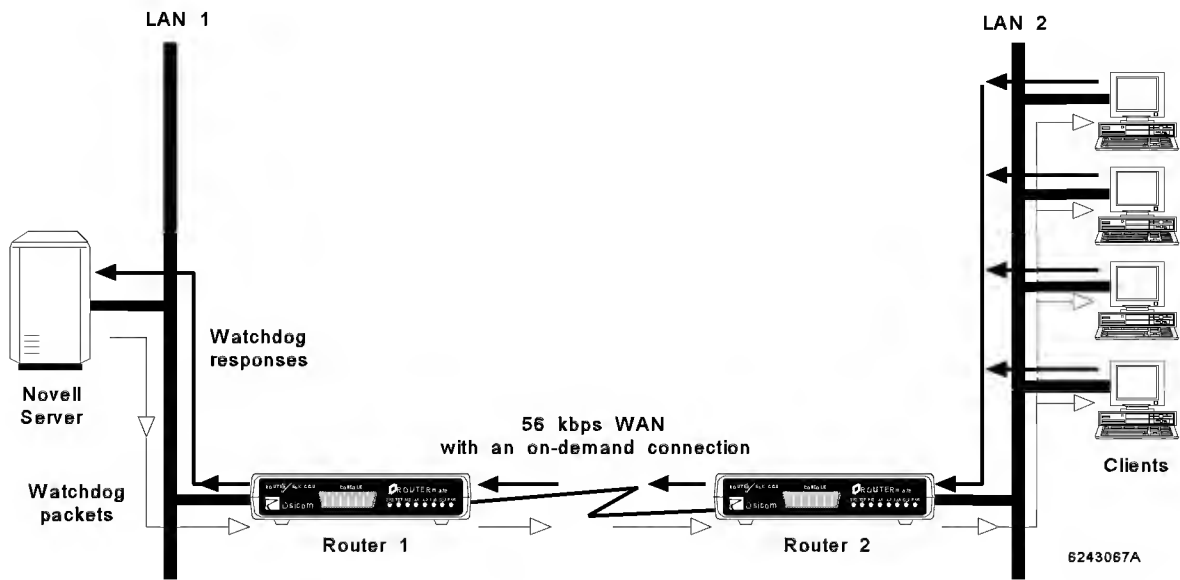


Figure B-14. Watchdog Spoofing Disabled

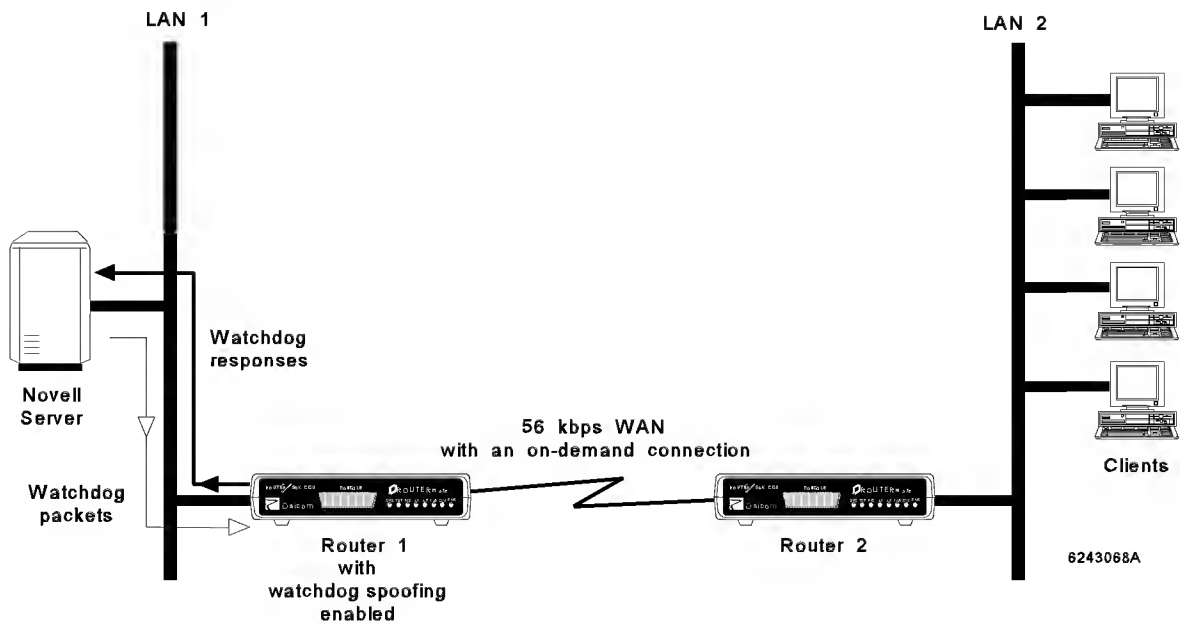


Figure B-15. Watchdog Spoofing Enabled

B.4.4 RIP

Routers in an IPX environment use the IPX Routing Information Protocol (RIP) to exchange routing information. The RIP used by IPX is different from the RIP used by IP, although the purposes of both are similar.

A router maintains a routing table that contains routing information for the entire network topology and is used to inform other routers about the network topology.

Each router advertises only to its adjacent routers. RIP messages advertise the information in the routing table to adjacent routers, and request information from adjacent routers, as follows:

- Upon power-up, an initial broadcast informs adjacent routers of networks that can be reached through the router.
- Upon power-up, an initial broadcast requests that adjacent routers provide routing information.
- Periodic broadcasts inform adjacent routers of current routes.
- A network topology change triggers an update to adjacent routers of current routes.

The routing table lets the router:

- Locate the fastest route.
- Retrieve routing information from other routers.
- Respond to requesting routers.
- Advertise the latest internetwork configuration.
- Advertise internetwork topology changes.

RIP defines the distance between a router and a destination network in *hops*. A network immediately adjacent to the local router is 1 hop away, a network that is reached by passing through 2 routers is 2 hops away, and so on.

IPX RIP also applies a *time tick* value to each route to rate the time required to pass data over the route. Specifically, there are 18.21 time ticks in a second, so a time tick equals approximately 1/18 second. If a router has two routes to the same network, the router selects the route with the lowest time tick value. If the time ticks are the same, the router selects the route with the lowest hop count. If the hop counts are the same, the router selects either of the two routes.

In Figure B-16, a data packet is sent from LAN 1 to LAN 4 via LAN 2 and LAN 3 even though the selected LAN path is 3 hops and the WAN path is only 1 hop; the LAN path is selected because the transmission time of 3 ticks for this path is less than the transmission time of 4 ticks over the link with a speed of 56 kbps (transmission speed on Ethernet=10 Mbps).

Each router sends RIP update packets that advertise the networks that can be reached via that router. The RIP update packets contain, for each network that can be reached via the advertising router, the IPX network number, the number of hops to the network, and the number of time ticks to the network.

Routers receiving the RIP messages update their routing tables accordingly and advertise to routers adjacent to them. The cumulative effect is that each router advertises to its neighbors all networks that can be reached through the router.

A path to a network that is learned over a particular interface is not advertised back over the same interface, since this would be redundant and could result in routing loops.

Devices other than routers can receive RIP messages and use them to update their routing tables, but only routers advertise their routes.

If a router does not receive an update from an adjacent router for by a pre-determined time, the router marks the routes served by the adjacent router as unusable and broadcasts the revised current table to adjacent routers. If an additional pre-determined time elapses and the route still has not been updated, it is deleted from the router's routing table.

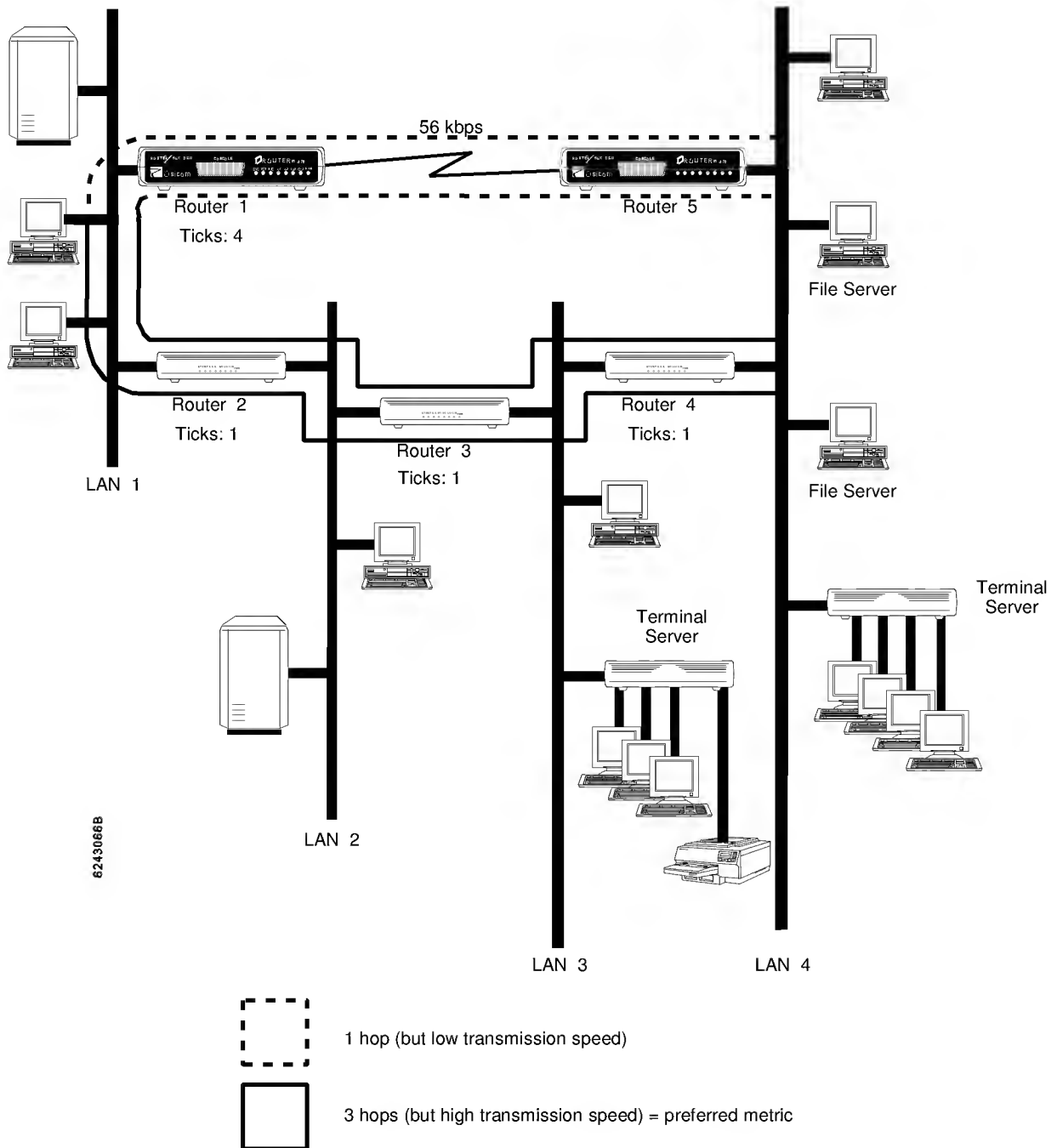


Figure B-16. IPX Transmission Over Fastest Path

B.4.5 RIP Filtering

IPX traffic can be filtered to keep certain types of routing information from being received or advertised.

For example, this might be done to:

- restrict access between certain networks.
- reduce the amount of routing information traffic (a particularly desirable feature when communicating over packet switched networks)

Ways in which a router might be configured to filter IPX traffic could include such filtering as the following:

- Specifying addresses from which RIP update packets will or will not be accepted.
- Specifying addresses to which RIP update packets will or will not be sent.

B.4.6 SAP

The Service Advertising Protocol (SAP) lets IPX devices advertise various Novell application services offered by such devices as file servers (file transfer), printer servers (print service) and gateways (protocol conversion).

A router has a SAP agent, which operates much like RIP. SAP agents collect and exchange service information about all the services available on the local network.

Table B-2 lists several commonly-used services.

Table B-2. Selected IPX Services	
SERVICE	SERVICE TYPE (OBJECT)
User	1
User Group	2
Print Queue	3
File Server	4
Job Server	5
Gateway	6
Print Server	7
Archive Queue	8
Archive Server	9
Job Queue	A
Administration	B
Remote Bridge Server 2	24
Bridge Server	26
TCP/IP Gateway	27
Archive Server SAP	2e
Advertising Print Server	47
Print Queue user	53
HP Laserjet	30c
Wildcard	FFFF

Workstations that require information about available services broadcast a SAP packet. For example, a workstation might broadcast "get nearest server;" the local SAP agent then responds with information about the nearest available file server.

SAP broadcasts are local broadcasts. They are initiated by servers once a minute and are received only by local SAP agents (i.e., the packets are not forwarded beyond the local segments).

SAP agents provide the following:

- Initiate workstation requests to get information about the name and address of the nearest server of a certain kind.
- Initiate router requests to get information about the names and addresses either of all servers, or of all servers of a certain kind on the internetwork.
- Send responses to requests originating from either a router or a workstation.
- Initiate periodic broadcasts by servers and routers.
- Update the accessible server information.

As with RIP routing, SAP routing keeps track of server addresses and the number of hops to the network on which the server is located. When a service is requested, it is routed along the fastest route.

Also, as with RIP, a SAP service is not advertised on the same port on which it was received since this would lead to redundancy.

B.4.7 SAP Filtering

Service information can be filtered to:

- Restrict access to servers by certain networks
- Reduce the amount of service information traffic (a particularly desirable feature when communicating over a low-speed WAN link)

Specifically, a router might advertise or accept SAP update packets according to network address, MAC address, service type, or a combination of these.

Table C-1. Console Interface

PIN	SIGNAL	DIRECTION
2	Transmit Data	Input
3	Receive Data	Output
5	Clear to Send	Output
6	Data Set Ready	Output
7	Signal Ground	—
8	Carrier Detect	Output



Table C-3. LAN Interface (10BaseT)

PIN	SIGNAL
1	Transmit Data (+)
2	Transmit Data (—)
3	Receive Data (+)
4	—
5	—
6	Receive Data (—)
7	—
8	—

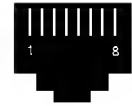


Table C-2. WAN 1 Interface

PIN	SIGNAL	DIRECTION
1	Receive	Input
2	Receive	Input
3	—	—
4	Transmit	Output
5	Transmit	Output
6	—	—
7	—	—
8	—	—

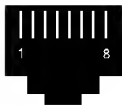


Table C-4. WAN 2 Interface (V.32 Modem)

PIN	SIGNAL
1	—
2	—
3	—
4	T Tip
5	R Ring
6	—
7	—
8	—

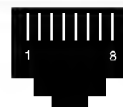


Table C-5. Router Cables		
DESCRIPTION	PART NUMBER	ORDER NUMBER
WAN 1 cable (included with unit)	DCA94511	CBE9451 (15 ft)
DDD line cable (included with WAN 2 integral V.32 dial modem option)	115-0414-001	CBE04141 (7 ft)

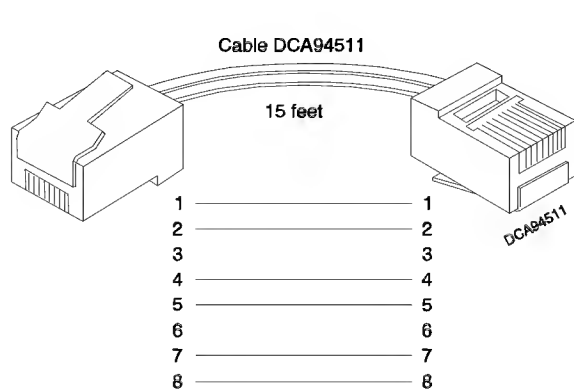
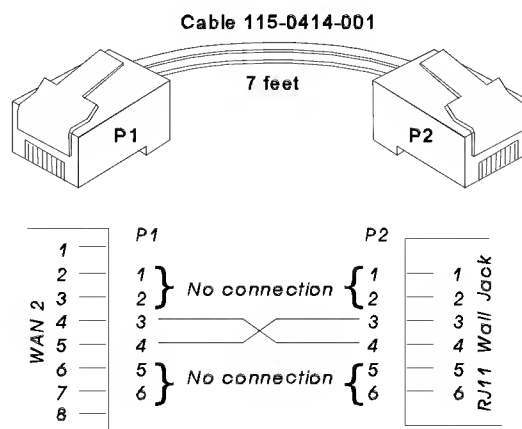


Figure C-1. WAN 1 Cable



NOTE: Cable 115-0414-001 is a 6-pin modular cable that connects the 8-pin WAN 2 interface to a 6-pin RJ11 wall jack. Cable connectors 3 and 4 connect to WAN 2 connectors 4 and 5, respectively.

Figure C-2. DDD Line Cable

Table D-1. Ordering Information	
DESCRIPTION	ORDER NUMBER
ROUTERmate Plus T1 (Router plus T1 CSU) IP and IPX router with bridging and integral T1 CSU; one 10Base-T LAN interface; one T1/FT1 WAN interface (WAN 1); 15-foot RJ48C line cable; wall-mount power transformer. Console, SNMP, and Telnet manageable. Includes base software, 4 MB RAM and 1 MB flash PROM.	RT1
Rackmount card version of above model.	RT1R
Order the options listed below by adding the order number to the base model order number. Example: RT1/B1/D1/E2 WAN 2 - Integral V.32 management modem; used for dial-in terminal management from a remote location. Includes 7-foot DDD line cable (115-0414-001). 4 MB SIMM memory module; increases unit's RAM to 8 MB total. High performance DES hardware encryption; used to add payload encryption on links up to T1 for PPP or Frame Relay; compatible with FPX4802/DES Frame Relay Encryptor.	B1 D1 E2
Management Enterprise MIB written in standard ASN.1 notation OsicomView network management for Windows. Contains Castle Rock's SNMPc management software plus BitView graphical user interface applications for Osicom's Internetworking products (3.5" DOS formatted disks). BitView graphical user interface (application only)	Free download from Osicom's Web site at http://www.osicom.com OsicomView OsicomView/Apps
Power Wall-mount transformer (spare for standalone unit)	550-0366-02

Table D-1. Ordering Information	
DESCRIPTION	ORDER NUMBER
MiniRack	
6-slot rack for ROUTERmate product family of routers and CSU/DSUs	RM-MiniRack
6-slot rack for ROUTERmate product family of routers and CSU/DSUs; includes 115 VAC power transformer and mounting brackets	RM-MiniRack/115
6-slot rack for ROUTERmate product family of routers and CSU/DSUs; includes redundant –48 VDC power supply and mounting brackets	RM-MiniRack/48V
115 VAC power transformer (spare)	905-7593-01
115 VAC power transformer rack mounting kit	415-0043-01
–48 VDC power module (spare)	905-7287-03
DES Master Key License	
Only one needed per network. For encryption option (E2); lets network administrator re-program, via terminal, both the master key and initial vector. License application provided to the customer at time of order.	DES-KEY-LIC
Manual	
Routermate Router Plus T1 CSU Installation and Operation.	918-6244

Table E-1. Routermate Plus T1 CSU Specifications (1 of 2)

ITEM	DESCRIPTION
Protocol Support Routing Bridging LAN frame types WAN 1 frame types	IP, IPX/SPX, RIP (IP), RIP/SAP (IPX/SPX) All popular LAN protocols, transparent bridging Type II, 802.2 (LLC), 802.3 (RAW), SNAP Frame relay, point-to-point (PPP)
Interfaces LAN WAN 1 Speed (NI) NI Format/Coding Timing Diagnostics WAN 2 (optional) Speed (NI)	Ethernet 10BaseT (RJ45) Integral T-1/Fractional T-1 CSU Nx56/64 kbps (RJ48C or RJ48X) up to 1,536 Mbps Auto Detect - D4, ESF, AMI, B8ZS Internal or Repeater V.54 w/integral 511 test generator Integral management modem V.32 (RJ11)
Management Console Speed (DCE) Telnet BootP TFTP (Client) SNMP Integral Modem (optional) Graphical User Interface (optional)	Asynchronous via RS-232 9600 bps (DB25) Built-in default IP address (user configurable) Configuration to Flash Operating system and configuration to Flash Private Enterprise MIB, MIB II, and Encryption MIB (Get, Set, Trap) V.32 (RJ11) Castle Rock <i>SNMPC</i>
Security (optional)	Integral DES Encryptor module
Memory 4 MB RAM 1 MB Flash PROM	SIMM upgrade to 8 MB Pre-loaded with router OS software
RFC Compliance	768, 791, 792, 793, 826, 854, 855, 862, 894, 903, 919, 922, 950, 951, 1010, 1058, 1155, 1157, 1166, 1212, 1213, 1315, 1332, 1350, 1490, 1542, 1552, 1570, 1634, 1638, 1661, 1723

Table E-1. Routermate Plus T1 CSU Specifications (2 of 2)

ITEM	DESCRIPTION
Power	
Standalone	Input: 120 VAC, 60 Hz; Output: 9 VAC @ 1 amp Input: 120 VAC, 60 Hz; Output: 9 VAC @ 2.1 amps (for units with optional encryption, compression, and WAN 2 interface installed)
6-slot MiniRack	AC module: Input: 120 VAC, 60 Hz; Output: 10 VAC @ 10 A DC module: Input: -48 VDC @ 6.25 A; Output: 8 to 12 VAC (9.5 nominal) @ 21.6 A max.
Dimensions	
Standalone	6.25" W x 9.6" D x 1.6" H
6-slot rack	17" W x 10.5" D x 3.5" (2U) H
Weight	
Standalone	2.3 lbs. fully-loaded (includes transformer)
Rack-mount card	1.4 lbs. (includes front and rear panels)
6-slot rack	7.7 lbs. empty (includes transformer)
Operating Temperature	32° to 104° F, 0° to 40° C
Relative Humidity	0% to 95%, non-condensing

The multipurpose labels for the Routermate and 6-slot MiniRack are found on the underside of the units. They are illustrated here for reference.

4800 SERIES ROUTER^{mate}™				
MAIN BOARD : SERIES HW/SW ___ / ___		FEATURE OPTIONS ☐ V.32bis ☐ ISDN U Compression : ☐ STD ☐ HI PERF Encryption : ☐ STD ☐ HI PERF ☐ PROP		SERIES HW ___ ___ ___
MEMORY OPTIONS : ☐ 4M <u>D</u> ram SIMM ☐ 2M <u>F</u> lash				
This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions : (1) this device may not cause harmful interference, and (2) this device must accept any interference that may cause undesired operation.				
This device complies with Part 68 of the FCC regulations. T1 CSU/DSU Reg No. : 1R5USA-23055-DE-N 56K CSU/DSU Reg No. : 1R5USA-23056-DE-N T1 DROP & INSERT Reg No. : 1R5USA-31067-DE-N ROUTER plus T1 CSU Reg No. : 1R5USA-24168-DE-N ROUTER plus 56K CSU Reg No. : 1R5USA-24165-DE-N V.32 MODEM Reg No. : 1R5USA-24168-DE-N Ringer Equivalence :		For T1 CSU/DSU : This Class A digital apparatus meets all requirements of the Canadian Interference Causing Equipment Regulations. Pour T1 CSU/DSU : Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel du Canada.		
POWER TRANSFORMERS ☐ P/N 550-0366-01 ☐ P/N 550-0366-02		BAR CODE LABEL		
LABEL		LABEL		
LABEL		LABEL		
MANUFACTURED BY				
 Osicom		Internetworking Division 9020 Junction Drive Annapolis Junction, MD 20701-1104, U.S.A.		
E-mail: info@osicom.com		http://www.osicom.com		
		179-0493-01 REV F		

Figure F-1. Multipurpose Label - Routermate

4800 SERIES ROUTER_{mate}[™]		905-7591-	179-0512-01 REV C																					
FOR 120VAC POWER USE PWR MOD 905-7593-01 120VAC 60Hz 1A	FOR 48VDC POWER USE PWR MOD 905-7598-01 48VDC 6.25A	Complies with Part 68 FCC Rules when used with the following registered equipment :																						
		<table border="1"> <thead> <tr> <th>Product</th> <th>Registration No.</th> <th>Ringer Equivalence</th> </tr> </thead> <tbody> <tr> <td>T1 CSU/DSU</td> <td>1R5USA-23055-DE-N</td> <td>N/A</td> </tr> <tr> <td>56K CSU/DSU</td> <td>1R5USA-23056-DE-N</td> <td>N/A</td> </tr> <tr> <td>T1 DROP & INSERT</td> <td>1R5USA-31067-DE-N</td> <td>N/A</td> </tr> <tr> <td>ROUTER plus T1 CSU</td> <td>1R5USA-24168-DE-N</td> <td>N/A</td> </tr> <tr> <td>ROUTER plus 56K CSU</td> <td>1R5USA-24165-DE-N</td> <td>N/A</td> </tr> <tr> <td>V.32 MODEM</td> <td>1R5USA-24168-DE-N</td> <td>N/A</td> </tr> </tbody> </table>		Product	Registration No.	Ringer Equivalence	T1 CSU/DSU	1R5USA-23055-DE-N	N/A	56K CSU/DSU	1R5USA-23056-DE-N	N/A	T1 DROP & INSERT	1R5USA-31067-DE-N	N/A	ROUTER plus T1 CSU	1R5USA-24168-DE-N	N/A	ROUTER plus 56K CSU	1R5USA-24165-DE-N	N/A	V.32 MODEM	1R5USA-24168-DE-N	N/A
		Product	Registration No.	Ringer Equivalence																				
T1 CSU/DSU	1R5USA-23055-DE-N	N/A																						
56K CSU/DSU	1R5USA-23056-DE-N	N/A																						
T1 DROP & INSERT	1R5USA-31067-DE-N	N/A																						
ROUTER plus T1 CSU	1R5USA-24168-DE-N	N/A																						
ROUTER plus 56K CSU	1R5USA-24165-DE-N	N/A																						
V.32 MODEM	1R5USA-24168-DE-N	N/A																						
AFFIX LABEL HERE AFFIX LABEL HERE		This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions : (1) This device may not cause harmful interference and (2) this device must accept any interference that may cause undesired operation.																						
MANUFACTURED BY 		Internetworking Division 9020 Junction Drive Annapolis Junction, MD 20701-1104, U.S.A.																						
http://www.osicom.com e-mail: info@osicom.com		FOR USE IN A RESTRICTED ACCESS LOCATION																						

Figure F-2. Multipurpose Label - MiniRack

Special-purpose diagnostics test certain hardware elements of the unit. The user can also view flash and system information.

NOTE

Diagnostic screens are intended to be used for manufacturing test purposes and error recovery when the full software image will not run.

When the unit is powered up, a prompt appears on the screen, as shown in Figure G-1. To enter the diagnostics, press **D** within 3 seconds. The Diagnostic Menu (Figure G-2) is displayed.

Type the letter of the desired operation to execute it.

```
ROUTERmate Plus T1 CSU Boot Diagnostics 2.x.xx
Copyright 1996-1997 Osicom Technologies, Inc.

Press D to run diagnostics
```

Figure G-1. Diagnostic Menu Prompt

When the user boots up and does not press **D**, the system verifies if the CRC in the software matches the CRC in the boot information database. If the CRC matches, the unit's software runs. If the CRC does not match, the bootcode will initiate BootP and try to automatically download a copy of the operating software (OS). If this is successful, the software will be run. If it fails, the router will reset.

```
ROUTERmate Plus T1 CSU Diagnostics

A - LED Test
B - RAM
C - Flash Test
D - TFTP Software Download
E - System Information
X - Exit

Select [A..E,X]:
```

Figure G-2. Diagnostic Menu

G.1	LED Test		G-2
G.2	RAM Test		G-2
G.3	Flash Test		G-3
G.4	TFTP Software Download	...	G-4
G.5	System Information		G-5

G.2 LED Test

The LED test checks the operation of the TST, ALM, W1, W2, and LAN LEDs. The LEDs will go ON and OFF in sequence for 5 to 6 seconds.

ROUTERmate Plus T1 CSU Diagnostics

- ```
A - LED Test
B - RAM
C - Flash Test
D - TFTP Software Download
E - System Information
X - Exit
```

Select [A..E,X]: A

## TESTING LEDS

### Figure G-3. LED Test

## G.4 RAM Test

Test A executes a minimal verification of RAM that non-destructively tests the read-write functions of the RAM. The test returns a result of Passed or Failed.

Tests **B**, **C**, and **D** execute a thorough verification of RAM. These tests overwrite RAM. The user is then prompted to press a key, after which the unit will reboot.

If the test is successful, the following message appears:

RAM Test Passed

If the test fails, the message below appears:

```
RAM Test Failed : Address = 0xffffffff
 (hex address)
```

## RAM Tests

- ```
A - Non-destructive RAM Test
B - 32-bit destructive RAM Test - Auto reboot
C - 16-bit destructive RAM Test - Auto reboot
D - 8-bit destructive RAM Test - Auto reboot
X - Exit
```

Select [A..D,X]: A

Testing RAM - Please Wait

```
RAM Test Passed
Press any key to continue:
```

Figure G-4. RAM Test

G.6 Flash Test

Select **A** to view information about the flash memory, as shown in Figure G-5.

```
Flash Tests

A - Flash Info
B - Erase Configuration Flash
X - Exit

Select [A..B,X]: A

Program Flash Information:

Make/Model  = AMD 29F040
Bus Width   = 16 bits
Flash Width  = 16 bits
Sector Size  = 128K
Total Size   = 1024K

Press any key to continue:
```

Figure G-5. Flash Test - Flash Info

Select **B** to remove the configuration in flash.

At the 'Enter password' prompt, enter the console password as it was configured on the Unit menu (Chapter 8). The configuration flash will not be erased unless the correct password is entered.

The unit returns to the Flash Tests screen. When the software is run, the unit uses the default configuration.

```
Flash Tests

A - Flash Info
B - Erase Configuration Flash
X - Exit

Select [A..B,X]: B

Enter password:
```

Figure G-6. Flash Test - Erase Configuration Flash

G.8 TFTP Software Download

When you select TFTP Software Download, the screen shown in Figure G-7 appears. Use this option to download the router's operating software or boot software from a specified TFTP server via the router's LAN interface.

The commands are intended for error recovery when the full software image will not run. The user can also upgrade the boot code via this screen.

Software downloads can only be performed across the LAN because the WAN is not operational when running from the boot sector.

NOTE

You can download through another router on the local LAN if you configure the LAN address of the other router as the Gateway Address.

When this screen is initially entered, the data displayed will be whatever was configured in the database.

You can configure the LAN IP Address, Subnet Mask, Server Address, Filename, and Gateway Address manually or via BootP. If you choose the latter, the new values will be displayed once the BootP reply is received.

Manually configure the LAN type for either TYPE II or SNAP.

Selecting **Initiate BOOTP** does not cause the download to start. After you are satisfied that all fields are set properly, press **[G]** to start a download of the operating software or **[H]** to start a download of the boot software.

NOTE

Any changes to the fields on the TFTP Download screen do not change the database in the main operating software.

Router Plus T1 CSU Code Download

A - Initiate BOOTP
B - Configure Lan IP Address: 128.1.128.1
C - Configure Lan IP Subnet Mask: 255.255.255.0
D - Configure Server Address: 125.0.0.103
E - Configure Filename: routerplus.txt
F - Configure Gateway Address: 0.0.0.0
G - Download Operational Code
H - Download Boot Code
I - Lan Frame Type: TYPE II
X - Exit

Select [A..I,X]:

Figure G-7. TFTP Software Download

G.10 System Information

Select System Information to view details of the unit's internal software and hardware components, as shown in Figure G-8.

If encryption is installed, the version will be displayed.

NOTE

The contents of the System Information screen is an example; your screen contents will be different.

System Information:

MAC address = 00:00:6d:13:57:90
Boot code version = 2.x.xx
Software size = 607K
Software checksum = 0xcf777318
DB version = 2
DB size = 76K

RAM size = 4M

SIMM: Installed
WAN2: Not Installed
Compression: Not Installed
V.32 Modem: Installed
Encryption: Not Installed

Press any key to continue:

Figure G-8. System Information

10BaseT interface 2-4, C-1

A

Action, configure for bridge static address 5-53

Address

aging time, bridge; configure 5-51

default route, IP 5-44

Ethernet (MAC), LAN interface 5-12

IP, configure 5-20

IPX internal network number, configure 5-49

IPX network number, configure 5-28

static (bridging) 5-52

static address, bridge; configure 5-52, 5-53

static route, IP; configure 5-46

trap client 9-2

Address resolution protocol B-16

Aging

address (bridging) 5-51

IPX RIP age timer, configure 5-30

SAP age timer, configure 5-30

Alarms, CSU 4-10

Annex D status (Frame Relay) 4-17, 4-19-21

ARP B-16

ARP table 4-43

Authentication traps, SNMP 9-2

Auto answer, dial-in management 7-2

Autolearn clients, SNMP 9-2

B

Bandwidth allocation 5-8

Bandwidth, WAN utilization 4-18

BCP status 4-31

BootP, download software G-1

Bridging

bridging table 4-56

enable, disable 5-17

global options, configure 5-50

status 4-49, 4-50

Broadcast (bridging) 5-50

C

Cables, part numbers C-2

Carrier registers 4-13

Clear channel operation 1-3

Client address, SNMP 9-2

Community strings, SNMP 9-2

Configuration

start up 2-7

Configuration and software update 6-1

Connectors 2-4

Console

interface 2-4

password 8-2

Counters, error (CSU) 4-9

CSU configuration 5-6

CSU status and test 4-8

Customer support 10-1

D

Data mode 5-10

Data rate 1-3

Data rate, CSU 5-9

DDD interface C-1

Default route

announce; enable, disable 5-25

global options, configure 5-44

Defaults restart 8-3

Diagnostic mode G-1

Diagnostic packets, IPX 5-31

Diagnostics

CSU 4-8

Diagnostics, start-up 3-3, G-1

Dial-in access 1-2

Dial-in management 2-6

DLCI status 4-20

DLCI, frame relay 5-17

Dotted decimal notation B-6

E

Encryption

frame relay; enable, disable 5-18

global options, configure 5-55

Encryption options 5-41

Equipment return and repair 10-1

Error counters, CSU 4-9

Error threshold (configure for frame relay) 5-14

ESF carrier loops 5-7

ESF data link 5-7

ESF operation 1-2

Ethernet B-2

F

File transfer 6-1

Filter mask, IPX SAP; configure 5-33

Filter State, IPX SAP; enable, disable 5-33

Filters, bridging

enable, disable 5-38

Transmit filter, configure 5-39

transmit filters 5-39

Filters, IP B-22

- enable, disable for port 5-25
- RIP Output Filter Table, configure 5-27
- RIP, configure 5-26
- Filters, IPX
 - RIP input/output filters 5-36
 - RIP/SAP input/output; enable, disable 5-32
 - SAP input, output filters; configure 5-33
- Firmware version 8-6
- Flash 2-9
- Flash boot G-1
- Frame Flooding, bridge; enable, disable 5-38
- Frame relay 5-14, B-4
 - encryption; enable, disable 5-18
 - protocol options, configure 5-14
 - protocol, configure 5-14
 - status, Annex D 4-17, 4-19-21
 - WAN status 4-17
- Frame Type
 - ethernet, configure 5-22
 - IPX, configure 5-28
- Full Enquiry Interval (configure for frame relay) .. 5-14

G

- Gap time, IPX RIP/SAP; configure 5-49
- Global configuration 5-43
- Glossary A-1

H

- Header, terminal screens 8-2
- Hop Count
 - too large, ICMP 4-37
 - too large, IP 4-37
 - too large, IPX 4-45
 - too large, Netbios 4-46
- Hop count (metric) 5-22
- Hops, IPX 4-54
- Host number B-6

I

- ICMP status 4-37
- Inactivity timeout, terminal 8-2
- Input datagrams 4-34
- Insert bit error 4-9
- Installation checklist 2-1
- Interface
 - configuration summary 5-11
 - map to port 5-17
 - speed, CSU 5-8
 - status summary screen 4-14
- Interface test, CSU 4-11
- Interfaces C-1

- LAN 2-4
- modem 2-4
- terminal 2-4
- WAN 1 2-4
- Internal Network Number, IPX; configure 5-49
- Inverse ARP
 - IP; enable, disable (WAN) 5-24
 - IPX; enable, disable 5-30
- IP address 5-20, B-6
- IP filters 5-25, B-22
- IP routes
 - default B-20
 - direct and learned B-20
 - static B-20
- IP routing B-6
 - ARP table 4-43
 - enable, disable 5-17
 - global options, configure 5-44
 - LAN 5-20
 - routing table 4-51
 - status 4-34
 - WAN 5-23
- IPCP status 4-29
- IPX B-23
- IPX routing
 - enable, disable 5-17
 - global options, configure 5-49
 - options, configure 5-28
 - RIP/SAP status 4-47
 - routing table 4-53
 - status 4-44
- IPX services table 4-55
- IPXCP status 4-30
- IPXWAN
 - enable, disable 5-28
 - status 4-48

K

- Key password 8-2
- Key Update Time, encryption; configure 5-55
- Keys; conventions & prompts 3-2

L

- LAN
 - configuration screen 5-12
 - status screen 4-15
- LAN interface 2-4, C-1
- LCP status 4-26
- LEDs 1-3, 2-3
- Line build out 5-7
- Line requirements 2-2

Line status, CSU	4-10
Local area network	B-2
Logoff	3-5
Loopback tests, CSU	4-8
Lower layer status	4-18

M

MAC address	
ARP	4-43
configure for bridging static address	5-53
LAN interface	5-12
Main menu	3-5
Maintenance services	10-1
Management methods	1-2
Management screen	9-2
Maximum Number of Configuration Requests, PPP;	
configure	5-54
Maximum Number of Termination Requests, PPP;	
configure	5-54
Maximum Transmission Unit (MTU); configure for IP	
(WAN)	5-24
Metric	
configure, default route	5-44
configure, IP	5-22
static route, IP; configure	5-46
MIB, enterprise	2-9
Modem	
connection	2-6
interface	2-4
Modem security	7-2
Modem, security password	7-2
Monitor events, configure (Frame Relay)	5-14
Multicast, transmit (bridge); enable, disable	5-38
Multipurpose label	F-1, F-2

N

Network address to filter, IPX SAP	5-33
Network number	B-6
Network number, IPX; configure	5-28
Next hop	
static route, IP; configure	5-46
NI coding	5-6
NI format	5-6
Node address to filter, IPX SAP; configure	5-34
Novell watchdog spoofing	5-32
Numbered	5-28

O

offset, bridge transmit filter; configure	5-39
Ordering information	D-1
Output datagrams	4-35

P

Part numbers, cables	C-2
Password	
console	2-5, 3-4
key (encryption)	8-2
remote dial-in management	2-6
terminal and telnet	8-2
Payload loop, CSU	4-9
Periodic RIP Timer, IPX; configure	5-28
Periodic SAP Timer, IPX; configure	5-30
Physical (MAC) address, for ARP	4-43
Ping	4-32
Point-to-Point protocol	B-3
Polling interval, configure (Frame Relay)	5-15
Polling Verification Timer Interval, configure (Frame	
Relay)	5-15
Port	
configuration	5-17
configuration summary	5-16
enable, disable	5-17
name, configure	5-17
negotiable options, LCP	4-28
static address, bridge; configure	5-53
status summary	4-22
status, frame relay	4-24
status, LAN	4-23
status, PPP	4-25
Port counters, IP	4-36
PPP	B-3
global options, configure	5-54
status, BCP	4-31
status, IPCP	4-29
status, IPXCP	4-30
status, LCP	4-26
protocol	
frame relay	5-14
LAN interface	5-12
PPP	5-14
WAN interface	5-13, 5-14

Q

Quick start procedure	2-7
-----------------------------	-----

R

R/O community string	9-2
R/W community string	9-2
Register summary	4-12
Remote dial-in access	2-6
Remote inband loops	5-7
Restart software, defaults	8-3
Restart Timer, PPP; configure	5-54
Restart, system	8-3
Return goods authorization	10-1
RIP	B-18
age timer	5-30
input filter, configure	5-26
input, output filters	5-36
neighbor list	5-44
RIP, IP	
enable, disable	5-21
input/output filters	5-27
listen only; enable, disable	5-26
output filter, configure	5-26
RIP, IPX	B-26
input/output filters	5-36
periodic update timer; configure	5-28
RIP, IPX status	4-47
Router summary	4-6

S

SAP	B-28
age timer	5-30
filters	B-29
input, output filters	5-33
input/output filters	5-33
status	4-47
Save to flash	3-5
Screen structure	
configuration	5-2
main menu	3-1
management	9-1
status and test	4-2
TFTP	6-1
unit	7-1, 8-1
Screens	
Annex D status	4-17, 4-19-21
ARP Table	4-43
Bandwidth Allocation	5-8
BCP Status	4-31
Bridging Global Configuration	5-50
Bridging Status	4-49
Bridging Table	4-56
Carrier Registers	4-13

CSU Status and Test	4-8
DLCI Status Table	4-20
Encryption Global Configuration	5-55
Encryption Options	5-41
Event Log	4-57
Global Configuration	5-43
ICMP Status	4-37
Interface Configuration (CSU)	5-9
Interface Configuration Summary	5-11
Interface Status	4-14
Interface Test	4-11
IP Global Configuration	5-44
IP RIP Input Filter Table	5-27
IP RIP Output Filter Table	5-27
IP Routing Table	4-51
IP Static Route	5-46
IP Static Route Table	5-46
IP Status	4-34
IPCP status	4-29
IPX Filters	5-31
IPX Global Configuration	5-49
IPX RIP/SAP Status	4-47
IPX Routing Table	4-53
IPX SAP Input Filter Table	5-33
IPX Services Table	4-55
IPX Status	4-44
IPXWAN Status	4-48
LAN Configuration	5-12
LAN Status	4-15
LCP Status	4-26
Lower Layer Status	4-18
Main Menu	3-5
Management	9-2
Ping/Trace Route	4-32
Port Bridging Status	4-50
Port Configuration	5-17
Port Configuration Summary	5-16
Port Counters	4-36
Port IP Filters (LAN)	5-25
Port IP Routing Options	5-20, 5-23
Port IPX Input Filter	5-36
Port IPX Output Filter	5-36
Port IPX RIP Input Filter Table	5-36
Port IPX RIP Output Filter Table	5-36
Port IPX Routing Options	5-28
Port IPX SAP Output Filter Table	5-33
Port Status	4-22, 4-23
PPP Global Configuration	5-54
Register Summary	4-12
Service Information	8-7
SNMP Status	4-41

-
- Screens (continued)
- Static Address Table, bridging 5-52
 - Static Address, bridging 5-52
 - System Information 8-6
 - System Restart 8-3
 - TCP and UDP Status 4-38
 - TCP Connection Table 4-40
 - TCP/IP Status 4-32
 - Transmit Filter 5-39
 - Transmit Filter Table 5-39
 - Unit 8-2
 - User Registers 4-13
 - WAN 1 Configuration 5-13
 - WAN 1 Protocol Options (Frame Relay) ... 5-14
 - WAN Status (Frame Relay) 4-17
 - Seconds in error 4-12
 - Seconds in test 4-12
 - Security password, dial-in management 7-2
 - Security password, modem 7-2
 - Serialization packets, IPX 5-31
 - Server name to filter, IPX SAP; configure 5-34
 - Server type to filter, IPX SAP; configure 5-34
 - Service Advertising Protocol (SAP) B-28
 - Service information 8-7
 - Service, phone number 10-1
 - SNMP 1-2, 2-5
 - client address 9-2
 - options 9-1
 - read only community string 9-2
 - read/write community string 9-2
 - status 4-41
 - Software update 6-1
 - Software version 8-6
 - Source quench 4-37
 - Specifications E-1
 - Speed, CSU 5-8
 - Start-up diagnostics 3-3, G-1
 - Start-up procedure, initial 2-7
 - Static address (route)
 - bridging, configure 5-52, 5-53
 - IP, announce routes 5-25
 - IP, configure 5-46
 - Static route table 5-44
 - Subnet mask B-7
 - configure for port 5-20
 - IP routing table 4-51
 - request from a device 4-38
 - static route, IP; configure 5-46
 - Subnet zero 5-45
 - Subnetworking 5-46, B-7
 - subnet mask 5-20
 - Support plans 10-1
 - System information screen 8-6
 - System restart 8-3
 - System time 8-2
- T**
- TCP connection table 4-40
 - TCP status 4-38
 - TCP/IP status 4-32
 - Telephone numbers 8-7, 10-1
 - Telnet 1-2
 - enable, disable 9-2
 - Terminal
 - configuration 3-3
 - connect 2-8
 - management 2-5
 - selection 3-3
 - Test patterns, CSU 4-9
 - Tests
 - diagnostics G-1
 - diagnostics, start-up G-1
 - loopback, CSU 4-8
 - TFTP (Trivial File Transfer Protocol) 6-1
 - TFTP software download G-4
 - Time, system 8-2
 - Timing, network 5-6
 - Trace route 4-32
 - Traceroute 4-32
 - Transmit broadcast, bridging 5-38
 - Transmit filter, bridge; configure 5-38
 - Transmit filter; bridging, configure 5-39
 - Transmit multicast, bridge; configure 5-38
 - Traps, SNMP 9-2, 9-3
 - Type 20 hop count 4-46
 - Type 20 packets, IPX 5-32
 - Type Value, bridge transmit filter; configure 5-39
- U**
- UDP status 4-38
 - Unit screen 8-2
 - Unnumbered 5-28
 - Upload/download files (TFTP) 6-4
 - User registers 4-13
 - Utilization, WAN 4-18
- V**
- V.32 modem 1-2
 - dial-in management 2-6
 - V.32 modem interface C-1
-

W

WAN

- protocol options, configure (frame relay) . . . 5-14
- WAN 1 interface 2-4, C-1
- WAN 2 interface 2-4
- WAN status screen 4-17, 4-21
- WAN to WAN forwarding (bridge) 5-51
- WAN utilization 4-18
- Watchdog packets 5-32
- Watchdog spoofing B-24